EXHIBIT A

THE SUPERIOR COURT OF CALIFORNIA
COUNTY OF SAN FRANCISCO

Case Number: CGC22601842
Title: MY CHOICE SOFTWARE, LLC, VS. SHOPIFY, INC., A CANADIAN CORPORATION ET AL
Cause of Action: COMMON COUNTS/OPEN BOOK ACCOUNT/COLLECTIONS
Generated: 2023-05-31 10:21 am

Register of Actions Parties Attorneys Calendar Payments Documents

Please Note: The "View" document links on this web page are valid until 10:31:22 am
After that, please refresh your web browser. (by pressing Command +R for Mac, pressing F5 for Windows or clicking the refresh button on your web browser)

Register of Actions

Show All entries Search:

Date	Proceedings	Document	Fee
2023-05-16	NOT REPORTED. COMPLEX LITIGATION CASE MANAGEMENT CONFERENCE SET FOR JUN-05-2023, IN DEPT. 304, IS CONTINUED TO JUN-23-2023, AT 1:30 PM, IN DEPT. 304, PER ORDER CONTINUING JUNE 5, 2023 CASE MANAGEMENT CONFERENCE, FILED ON MAY-16-2023. (D304)		
2023-05-16	ORDER CONTINUING JUNE 5, 2023 CASE MANAGEMENT CONFERENCE (TRANS# 70028342)	View	
2023-05-12	NOTICE AND ACKNOWLEDGMENT OF RECEIPT, SIGNED MAY-12-2023, SERVED APR-24-2023 (TRANSACTION ID # 100199845) FILED BY PLAINTIFF MY CHOICE SOFTWARE, LLC, A CALIFORNIA LIMITED LIABILITY COMPANY, INDIVIDUALLY, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED AS TO DEFENDANT SHOPIFY (USA) INC., A DELAWARE CORPORATION	View	
2023-05-12	NOTICE AND ACKNOWLEDGMENT OF RECEIPT, SIGNED MAY-12-2023, SERVED APR-24-2023 (TRANSACTION ID # 100199794) FILED BY PLAINTIFF MY CHOICE SOFTWARE, LLC, A CALIFORNIA LIMITED LIABILITY COMPANY, INDIVIDUALLY, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED AS TO DEFENDANT SHOPIFY, INC., A CANADIAN CORPORATION	View	
2023-05-12	NOTICE AND ACKNOWLEDGMENT OF RECEIPT, SIGNED MAY-12-2023, SERVED APR-24-2023 (TRANSACTION ID # 100199792) FILED BY PLAINTIFF MY CHOICE SOFTWARE, LLC, A CALIFORNIA LIMITED LIABILITY COMPANY, INDIVIDUALLY, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED AS TO DEFENDANT SHOPIFY (USA) INC., A DELAWARE CORPORATION	View	
2023-03-02	NOT REPORTED. COMPLEX LITIGATION CASE MANAGEMENT CONFERENCE SET FOR MAR-07-2023, IN DEPT. 304, IS CONTINUED TO JUN-05-2023, AT 10:00 AM, IN DEPT. 304, PER ORDER CONTINUING MARCH 7, 2023 CASE MANAGEMENT CONFERENCE, DATED MAR-02-2023. (D304)		
2023-03-02	ORDER CONTINUING MARCH 7, 2023 CASE MANAGEMENT CONFERENCE (TRANS# 69262576)	View	
2023-01-26	INITIAL CASE MANAGEMENT CONFERENCE OF FEB-21-2023 CONTINUED TO MAR-07-2023 AT 10:00 AM IN DEPT. 304 ON COURTS OWN MOTION. NOTICE SENT BY COURT. (TRANSACTION 69008362)	View	
2022-12-28	ORDER GRANTING COMPLEX DESIGNATION AND FOR SINGLE ASSIGNMENT TO JUDGE ETHAN P. SCHULMAN FOR ALL PURPOSES. CASE MANAGEMENT CONFERENCE SET FOR FEB-21-2023 AT 10:00 AM IN DEPT. 304. FEB-15-2023 CASE MANAGEMENT CONFERENCE IN DEPT. 610 IS OFF CALENDAR. NOTICE SENT BY COURT.	View	
2022-12-08	APPLICATION FOR APPROVAL OF COMPLEX LITIGATION DESIGNATION (TRANSACTION ID # 68546008) FILED BY PLAINTIFF MY CHOICE SOFTWARE, LLC, A CALIFORNIA LIMITED LIABILITY COMPANY, INDIVIDUALLY, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED	View	$60.00
2022-12-05	ORDER DENYING COMPLEX DESIGNATION FOR FAILURE TO FILE APPLICATION REQUESTING DESIGNATION	View	
2022-10-12	NOTICE OF RELATED CASE (TRANSACTION ID # 68246634) FILED BY PLAINTIFF MY CHOICE SOFTWARE, LLC, A CALIFORNIA LIMITED LIABILITY COMPANY, INDIVIDUALLY, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED	View	
2022-09-16	NOTICE TO PLAINTIFF	View	
2022-09-16	CIVIL CASE COVERSHEET FILED (TRANSACTION ID # 68117922) FILED BY PLAINTIFF MY CHOICE SOFTWARE, LLC, A CALIFORNIA LIMITED LIABILITY COMPANY, INDIVIDUALLY, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED	View	

Date	Proceedings	Document	Fee
2022-09-16	COMMON COUNTS/OPEN BOOK ACCOUNT/COLLECTIONS, COMPLAINT (TRANSACTION ID # 68117922) FILED BY PLAINTIFF MY CHOICE SOFTWARE, LLC, A CALIFORNIA LIMITED LIABILITY COMPANY, INDIVIDUALLY, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED AS TO DEFENDANT SHOPIFY, INC., A CANADIAN CORPORATION SHOPIFY (USA) INC., A DELAWARE CORPORATION TASKUS INC., A DELAWARE CORPORATION DOES 1 THROUGH 100, INCLUSIVE NO SUMMONS ISSUED, JUDICIAL COUNCIL CIVIL CASE COVER SHEET NOT FILED CASE MANAGEMENT CONFERENCE SCHEDULED FOR FEB-15-2023 PROOF OF SERVICE DUE ON NOV-15-2022 CASE MANAGEMENT STATEMENT DUE ON JAN-23-2023 COMPLEX LITIGATION ASSIGNMENT REQUESTED BY FILING PARTIES; FEE INCLUDED IN FILING FEE	View	$1435.00

Showing 1 to 15 of 15 entries

Previous 1 Next

SUM-100

SUMMONS
(CITACION JUDICIAL)

FOR COURT USE ONLY
(SOLO PARA USO DE LA CORTE)

NOTICE TO DEFENDANT:
(AVISO AL DEMANDADO):
SHOPIFY, INC., a Canadian Corporation; SHOPIFY (USA) INC., a Delaware Corporation; and DOES 1 through 100, inclusive

YOU ARE BEING SUED BY PLAINTIFF:
(LO ESTÁ DEMANDANDO EL DEMANDANTE):
MY CHOICE SOFTWARE, LLC, a California Limited Liability Company, individuallym and on behalf of all others similarly situated

NOTICE! You have been sued. The court may decide against you without your being heard unless you respond within 30 days. Read the information below.

You have 30 CALENDAR DAYS after this summons and legal papers are served on you to file a written response at this court and have a copy served on the plaintiff. A letter or phone call will not protect you. Your written response must be in proper legal form if you want the court to hear your case. There may be a court form that you can use for your response. You can find these court forms and more information at the California Courts Online Self-Help Center (*www.courtinfo.ca.gov/selfhelp*), your county law library, or the courthouse nearest you. If you cannot pay the filing fee, ask the court clerk for a fee waiver form. If you do not file your response on time, you may lose the case by default, and your wages, money, and property may be taken without further warning from the court.

There are other legal requirements. You may want to call an attorney right away. If you do not know an attorney, you may want to call an attorney referral service. If you cannot afford an attorney, you may be eligible for free legal services from a nonprofit legal services program. You can locate these nonprofit groups at the California Legal Services Web site (*www.lawhelpcalifornia.org*), the California Courts Online Self-Help Center (*www.courtinfo.ca.gov/selfhelp*), or by contacting your local court or county bar association. **NOTE:** The court has a statutory lien for waived fees and costs on any settlement or arbitration award of $10,000 or more in a civil case. The court's lien must be paid before the court will dismiss the case.

¡AVISO! *Lo han demandado. Si no responde dentro de 30 días, la corte puede decidir en su contra sin escuchar su versión. Lea la información a continuación.*

*Tiene 30 DÍAS DE CALENDARIO después de que le entreguen esta citación y papeles legales para presentar una respuesta por escrito en esta corte y hacer que se entregue una copia al demandante. Una carta o una llamada telefónica no lo protegen. Su respuesta por escrito tiene que estar en formato legal correcto si desea que procesen su caso en la corte. Es posible que haya un formulario que usted pueda usar para su respuesta. Puede encontrar estos formularios de la corte y más información en el Centro de Ayuda de las Cortes de California (*www.sucorte.ca.gov*), en la biblioteca de leyes de su condado o en la corte que le quede más cerca. Si no puede pagar la cuota de presentación, pida al secretario de la corte que le dé un formulario de exención de pago de cuotas. Si no presenta su respuesta a tiempo, puede perder el caso por incumplimiento y la corte le podrá quitar su sueldo, dinero y bienes sin más advertencia.*

*Hay otros requisitos legales. Es recomendable que llame a un abogado inmediatamente. Si no conoce a un abogado, puede llamar a un servicio de remisión a abogados. Si no puede pagar a un abogado, es posible que cumpla con los requisitos para obtener servicios legales gratuitos de un programa de servicios legales sin fines de lucro. Puede encontrar estos grupos sin fines de lucro en el sitio web de California Legal Services, (*www.lawhelpcalifornia.org*), en el Centro de Ayuda de las Cortes de California, (*www.sucorte.ca.gov*) o poniéndose en contacto con la corte o el colegio de abogados locales. AVISO: Por ley, la corte tiene derecho a reclamar las cuotas y los costos exentos por imponer un gravamen sobre cualquier recuperación de $10,000 ó más de valor recibida mediante un acuerdo o una concesión de arbitraje en un caso de derecho civil. Tiene que pagar el gravamen de la corte antes de que la corte pueda desechar el caso.*

The name and address of the court is:
(El nombre y dirección de la corte es):
San Francisco County Superior Courthouse
400 McAllister St., San Francisco, CA 94102

CASE NUMBER:
(Número del Caso):

The name, address, and telephone number of plaintiff's attorney, or plaintiff without an attorney, is:
(El nombre, la dirección y el número de teléfono del abogado del demandante, o del demandante que no tiene abogado, es):
Richard E. Quintilone II (SBN 200995) Jeffrey T. Green (SBN 330065)
Quintilone & Associates, 22974 El Toro, Suite 100, Lake Forest, CA 92630
Telephone No.: 949-458-9675
Fax No.: 949-458-9679

DATE: *(Fecha)*
Clerk, by *(Secretario)* _____ , Deputy *(Adjunto)*

(For proof of service of this summons, use Proof of Service of Summons *(form POS-010).)*
(Para prueba de entrega de esta citatión use el formulario Proof of Service of Summons, *(POS-010)).*

[SEAL]

NOTICE TO THE PERSON SERVED: You are served
1. ☐ as an individual defendant.
2. ☐ as the person sued under the fictitious name of *(specify):*
3. ☐ on behalf of *(specify):*

under: ☐ CCP 416.10 (corporation) ☐ CCP 416.60 (minor)
☐ CCP 416.20 (defunct corporation) ☐ CCP 416.70 (conservatee)
☐ CCP 416.40 (association or partnership) ☐ CCP 416.90 (authorized person)
☐ other *(specify):*

4. ☐ by personal delivery on *(date)*:

Form Adopted for Mandatory Use
Judicial Council of California
SUM-100 [Rev. July 1, 2009]

SUMMONS

Code of Civil Procedure §§ 412.20, 465
www.courtinfo.ca.gov
LexisNexis® Automated California Judicial Council Forms

CM-010

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name, state bar number, and address)
Richard E. Quintilone (SBN 200995) Jeffrey T. Green (SBN 330065); Kyle J. Gallego (PL513245)
QUINTILONE & ASSOCIATES
22974 El Toro Road Ste 100, Lake Forest, CA 92630
TELEPHONE NO.: (949) 458-9675 FAX NO.: (949) 458-9679
ATTORNEY FOR (Name): Plaintiff MY CHOICE SOFTWARE, LLC, et al.

FOR COURT USE ONLY

ELECTRONICALLY
FILED
Superior Court of California, County of San Francisco
09/16/2022
Clerk of the Court
BY: JEFFREY FLORES
Deputy Clerk

SUPERIOR COURT OF CALIFORNIA, COUNTY OF Orange
STREET ADDRESS: 400 McAllister St.
MAILING ADDRESS: 400 McAllister St.
CITY AND ZIP CODE: San Francisco, CA 94102
BRANCH NAME: San Francisco Superior Courthouse

CASE NAME:
My Choice Software, LLC, et al. v. Shopify, Inc., et al.

CIVIL CASE COVER SHEET

[X] **Unlimited** (Amount demanded exceeds $25,000) [ ] **Limited** (Amount demanded is $25,000 or less)

Complex Case Designation

[ ] Counter [ ] Joinder

Filed with first appearance by defendant (Cal. Rules of Court, rule 1811)

CASE NUMBER: **CGC-22-601842**

JUDGE:

DEPT.:

All five (5) items below must be completed (see instructions on page 2).

1. Check **one** box below for the case type that best describes this case:

Auto Tort
- [ ] Auto (22)
- [ ] Uninsured motorist (46)

Other PI/PD/WD (Personal Injury/Property Damage/Wrongful Death) Tort
- [ ] Asbestos (04)
- [ ] Product liability (24)
- [ ] Medical malpractice (45)
- [ ] Other PI/PD/WD (23)

Non-PI/PD/WD (Other) Tort
- [ ] Business tort/unfair business practice (07)
- [ ] Civil rights (08)
- [ ] Defamation (13)
- [ ] Fraud (16)
- [ ] Intellectual property (19)
- [ ] Professional negligence (25)
- [ ] Other non-PI/PD/WD tort (35)

Employment
- [ ] Wrongful termination (36)
- [ ] Other employment (15)

Contract
- [X] Breach of contract/warranty (06)
- [ ] Collections (09)
- [ ] Insurance coverage (18)
- [ ] Other contract (37)

Real Property
- [ ] Eminent domain/Inverse condemnation (14)
- [ ] Wrongful eviction (33)
- [ ] Other real property (26)

Unlawful Detainer
- [ ] Commercial (31)
- [ ] Residential (32)
- [ ] Drugs (38)

Judicial Review
- [ ] Asset forfeiture (05)
- [ ] Petition re: arbitration award (11)
- [ ] Writ of mandate (02)
- [ ] Other judicial review (39)

Provisionally Complex Civil Litigation (Cal. Rules of Court, rules 1800–1812)
- [ ] Antitrust/Trade regulation (03)
- [ ] Construction defect (10)
- [ ] Mass tort (40)
- [ ] Securities litigation (28)
- [ ] Environmental /Toxic tort (30)
- [ ] Insurance coverage claims arising from the above listed provisionally complex case types (41)

Enforcement of Judgment
- [ ] Enforcement of judgment (20)

Miscellaneous Civil Complaint
- [ ] RICO (27)
- [ ] Other complaint *(not specified above)* (42)

Miscellaneous Civil Petition
- [ ] Partnership and corporate governance (21)
- [ ] Other petition *(not specified above)* (43)

2. This case [X] is [ ] is not complex under rule 1800 of the California Rules of Court. If the case is complex, mark the factors requiring exceptional judicial management:
   a. [X] Large number of separately represented parties
   b. [X] Extensive motion practice raising difficult or novel issues that will be time-consuming to resolve
   c. [X] Substantial amount of documentary evidence
   d. [X] Large number of witnesses
   e. [ ] Coordination with related actions pending in one or more courts in other counties, states or countries, or in a federal court
   f. [ ] Substantial post-judgment judicial supervision
3. Type of remedies sought *(check all that apply)*:
   a. [X] monetary b. [X] nonmonetary; declaratory or injunctive relief c. [X] punitive
4. Number of causes of action *(specify)*: 8; See Attached Complaint.
5. This case [ ] is [X] is not a class action suit.

Date: September 16, 2022

JEFFREY T. GREEN, ESQ.
(TYPE OR PRINT NAME)

▶ _____
(SIGNATURE OF PARTY OR ATTORNEY FOR PARTY)

NOTICE
- Plaintiff must file this cover sheet with the first paper filed in the action or proceeding (except small claims cases or cases filed under the Probate, Family, or Welfare and Institutions Code). (Cal. Rules of Court, rule 201.8.) Failure to file may result in sanctions.
- File this cover sheet in addition to any cover sheet required by local court rule.
- If this case is complex under rule 1800 et seq. of the California Rules of Court, you must serve a copy of this cover sheet on **all** other parties to the action or proceeding.
- Unless this is a complex case, this cover sheet will be used for statistical purposes only.

Form Adopted for Mandatory Use
Judicial Council of California
CM-010 [Rev. July 1, 2003]

CIVIL CASE COVER SHEET

Cal. Rules of Court, rules 201.8, 1800–1812
Standards of Judicial Administration § 19
www.courtinfo.ca.gov

LexisNexis™ Automated California Judicial Council Forms

INSTRUCTIONS ON HOW TO COMPLETE THE COVER SHEET

To Plaintiffs and Others Filing First Papers

If you are filing a first paper (for example, a complaint) in a civil case, you **must** complete and file, along with your first paper, the *Civil Case Cover Sheet* contained on page 1. This information will be used to compile statistics about the types and numbers of cases filed. You must check **all five** items on the sheet. In item 1, you must check **one** box for the case type that best describes the case. If the case fits both a general and a more specific type of case listed in item 1, check the more specific one. If the case has multiple causes of action, check the box that best indicates the **primary** cause of action. To assist you in completing the sheet, examples of the cases that belong under each case type in item 1 are provided below. A cover sheet must be filed only with your initial paper. You do not need to submit a cover sheet with amended papers. Failure to file a cover sheet with the first paper filed in a civil case may subject a party, its counsel, or both to sanctions under rules 201.8(c) and 227 of the California Rules of Court.

To Parties in Complex Cases

In complex cases only, parties must also use the *Civil Case Cover Sheet* to designate whether the case is complex. If a plaintiff believes the case is complex under rule 1800 of the California Rules of Court, this must be indicated by completing the appropriate boxes in items 1 and 2. If a plaintiff designates a case as complex, the cover sheet must be served with the complaint on all parties to the action. A defendant may file and serve no later than the time of its first appearance a joinder in the plaintiff's designation, a counter-designation that the case is not complex, or, if the plaintiff has made no designation, a designation that the case is complex.

CASE TYPES AND EXAMPLES

Auto Tort
- Auto (22)–Personal Injury/Property Damage/Wrongful Death
- Uninsured Motorist (46) *(if the case involves an uninsured motorist claim subject to arbitration, check this item instead of Auto)*

Other PI/PD/WD (Personal Injury/ Property Damage/Wrongful Death) Tort
- Asbestos (04)
  - Asbestos Property Damage
  - Asbestos Personal Injury/ Wrongful Death
- Product Liability *(not asbestos or toxic/environmental)* (24)
- Medical Malpractice (45)
  - Medical Malpractice–Physicians & Surgeons
  - Other Professional Health Care Malpractice
- Other PI/PD/WD (23)
  - Premises Liability (e.g., slip and fall)
  - Intentional Bodily Injury/PD/WD (e.g., assault, vandalism)
  - Intentional Infliction of Emotional Distress
  - Negligent Infliction of Emotional Distress
  - Other PI/PD/WD

Non-PI/PD/WD (Other) Tort
- Business Tort/Unfair Business Practice (07)
- Civil Rights (e.g., discrimination, false arrest) *(not civil harassment)* (08)
- Defamation (e.g., slander, libel) (13)
- Fraud (16)
- Intellectual Property (19)
- Professional Negligence (25)
  - Legal Malpractice
  - Other Professional Malpractice *(not medical or legal)*
- Other Non-PI/PD/WD Tort (35)

Employment
- Wrongful Termination (36)
- Other Employment (15)

Contract
- Breach of Contract/Warranty (06)
  - Breach of Rental/Lease Contract *(not unlawful detainer or wrongful eviction)*
  - Contract/Warranty Breach–Seller Plaintiff *(not fraud or negligence)*
  - Negligent Breach of Contract/ Warranty
  - Other Breach of Contract/Warranty
- Collections (e.g., money owed, open book accounts) (09)
  - Collection Case–Seller Plaintiff
  - Other Promissory Note/Collections Case
- Insurance Coverage *(not provisionally complex)* (18)
  - Auto Subrogation
  - Other Coverage
- Other Contract (37)
  - Contractual Fraud
  - Other Contract Dispute

Real Property
- Eminent Domain/Inverse Condemnation (14)
- Wrongful Eviction (33)
- Other Real Property (e.g., quiet title) (26)
  - Writ of Possession of Real Property
  - Mortgage Foreclosure
  - Quiet Title
  - Other Real Property *(not eminent domain, landlord/tenant, or foreclosure)*

Unlawful Detainer
- Commercial *(31)*
- Residential *(32)*
- Drugs *(38) (if the case involves illegal drugs, check this item; otherwise, report as Commercial or Residential.)*

Judicial Review
- Asset Forfeiture (05)
- Petition Re: Arbitration Award (11)
- Writ of Mandate (02)
  - Writ–Administrative Mandamus
  - Writ–Mandamus on Limited Court Case Matter
  - Writ–Other Limited Court Case Review
- Other Judicial Review (39)
  - Review of Health Officer Order
  - Notice of Appeal–Labor Commissioner Appeals

Provisionally Complex Civil Litigation (Cal. Rules of Court Rule 1800-1812)
- Antitrust/Trade Regulation (03)
- Construction Defect (10)
- Claims Involving Mass Tort (40)
- Securities Litigation (28)
- Toxic Tort/Environmental (30)
- Insurance Coverage Claims *(arising from provisionally complex case type listed above)* (41)

Enforcement of Judgment
- Enforcement of Judgment (20)
  - Abstract of Judgment (Out of County
  - Confession of Judgment *(non-domestic relations)*
  - Sister State Judgment
  - Administrative Agency Award *(not unpaid taxes)*
  - Petition/Certification of Entry of Judgment on Unpaid Tax
  - Other Enforcement of Judgment Case

Miscellaneous Civil Complaint
- RICO (27)
- Other Complaint *(not specified above)* (42)
  - Declaratory Relief Only
  - Injunctive Relief Only *(non-harassment)*
  - Mechanics Lien
  - Other Commercial Complaint Case *(non-tort/non-complex)*
  - Other Civil Complaint *(non-tort/non-complex)*

Miscellaneous Civil Petition
- Partnership and Corporate Governance (21)
- Other Petition *(not specified above)* (43)
  - Civil Harassment
  - Workplace Violence
  - Elder/Dependent Adult Abuse
  - Election Contest
  - Petition for Name Change
  - Petition for Relief from Late Claim
  - Other Civil Petition

RICHARD E. QUINTILONE II (SBN 200995)
JEFFREY T. GREEN (SBN 330065)
KYLE J. GALLEGO (PL 513245)
QUINTILONE & ASSOCIATES
22974 EL TORO ROAD, SUITE 100
LAKE FOREST, CA 92630
TELEPHONE: (949) 458-9675
FACSIMILE: (949) 458-9679
E-MAIL: REQ@QUINTLAW.COM; JTG@QUINTLAW.COM

Attorneys for Plaintiff, MY CHOICE SOFTWARE, LLC, a California Limited Liability Company, individually, and on behalf of all others similarly situated.

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SAN FRANCISCO

CGC-22-601842

MY CHOICE SOFTWARE, LLC, a California Limited Liability Company, individually, and on behalf of all others similarly situated;

Plaintiff,

vs.

SHOPIFY, INC., a Canadian Corporation; SHOPIFY (USA) INC., a Delaware Corporation; TASKUS INC., a Delaware Corporation, and DOES 1 through 100, inclusive,

Defendants.

Case No.:

CLASS ACTION

Assigned For All Purposes To:
Hon.
Dept.:

CLASS ACTION COMPLAINT FOR:

1. **NEGLIGENCE;**
2. **BREACH OF CONTRACT;**
3. **BREACH OF IMPLIED CONTRACT;**
4. **BREACH ON CONFIDENCE;**
5. **UNFAIR AND UNLAWFUL BUSINESS PRACTICES;**
6. **VIOLATION OF CLRA;**
7. **DECEIT BY CONCEALMENT; AND**
8. **VIOLATION OF CUSTOMER RECORDS ACT;**

DEMAND FOR JURY TRIAL

Plaintiff MY CHOICE SOFTWARE, LLC brings this action on behalf of itself and all others similarly situated against SHOPIFY INC. and SHOPIFY (USA) INC. (collectively, "Shopify") and . TASKUS INC, a Delaware Corporation (Collectively "Defendants") Plaintiff's allegations against Shopify are based upon information and belief and upon investigation of Plaintiff's counsel, except for allegations specifically pertaining to Plaintiff, which are based upon Plaintiff's personal knowledge.

I. INTRODUCTION

1. Shopify is an e-commerce platform that enables merchants to easily sell products online. Many of Shopify's customers are merchants who operate websites and mobile applications, such as IABMFG. Shopify created software code to enable merchants to integrate Shopify's payment forms into their applications. To that end, Shopify provides comprehensive documentation to its merchant customers, describing how to integrate payment forms into their websites and applications using the Shopify code, including how to omit Shopify branding such that the form appears to the consumer to belong to the merchant's website.

2. In fact, despite the appearance to consumers that their payment information is being sent to the merchant, it is intercepted by Shopify. When a merchant integrates the Shopify software code into a website or mobile application, consumers who desire to pay for a product or service are presented with Shopify payment forms, which are created by Shopify. The payment forms require the consumer to provide a variety of sensitive information, such as:

a. Name;

b. Address;

c. Telephone number;

d. Email address; and

e. Complete credit card information, including cvc.

3. Shopify also collects and, by sharing the data with its payment processor, Stripe, Inc., indefinitely stores sensitive information about consumers using its payment form such as:

a. The consumers' internet IP addresses;

b. The brand and model of the consumer's computers or electronic devices;

c. The identities of the consumer's browsers;

d. The operating systems that the consumer's devices were using; and

e. The item(s) purchased by the consumer from the merchants' websites.

4. Although consumers using merchants' websites and mobile applications reasonably expect that they are communicating directly with the merchant, Shopify's software code is designed to enable Shopify's computer network to intercept those communications and redirect them to Shopify's computer network. Shopify, however, designed its payment forms to omit all Shopify branding. Accordingly, the consumer has no idea that Shopify is involved in the transaction in any way, let alone that Shopify will be obtaining, transmitting, storing, and/or evaluating the consumer's sensitive communications and information.

5. The Shopify code also surreptitiously installs tracking cookies on consumers' computers and mobile devices, which enable Shopify to identify a particular consumer and track his or her activities across its entire merchant network, enabling Shopify to gather even more sensitive data about the consumer including, without limitation, (i) the number of declined cards that the consumer has used with Shopify merchants; (ii) how long ago one of the consumer's cards was last declined; (iii) whether the consumer had ever disputed a previous Shopify charge; (iv) whether any previous early fraud warnings were associated with the consumer; (v) the percentage of transactions that were authorized for the consumer over time; and (vi) the cards and other payment methods associated with the consumer's IP address. Shopify accomplishes this, in part, by using the payment processing product provided by Stripe.

6. Shopify does not use consumers' private information simply for the purposes of processing the payments in question. Instead, using its own database as well as Stripe, Shopify indefinitely stores the information and correlates all payments from the consumer made across its entire platform. Although Shopify does not inform consumers of this, much of this private information is provided to other merchants, including those who do not use the Shopify platform. For example, on information and belief, once a consumer has submitted a payment for a purchase from IABMFG, any of Stripe's millions of other merchant customers will then be able to use Stripe's Radar product to access the consumer's private information pertaining to that payment, as well as any other payment that Shopify processed for that consumer, in a profile for that consumer.

///

7. Consumers using Shopify payment forms on merchant websites are not required to consent to any of Shopify's activities, and therefore are unaware that: (i) Shopify will intercept communications that consumers believe are being sent exclusively to merchants; (ii) its software code is causing their devices to connect to Shopify's computer servers; (iii) Shopify is accessing consumers' data by placing tracking cookies on their devices; (iv) its software code is rendering the payment forms that are displayed to consumers; (v) the sensitive information in the payment forms will be sent to Shopify; (vi) sensitive information not expressly inputted by the consumer—such as IP address, operating system, geolocation data, and item(s) purchased—will also be collected from the consumer by Shopify; (vii) Shopify will indefinitely store that sensitive information using its own database and Stripe; (viii) consumers' private information will be used to create profiles of consumers, which could subsequently be communicated to other merchants on and off the Shopify network; (ix) Shopify will track consumers' behavior across over more than one million websites; and (x) consumers' sensitive information could be made available to millions of merchants who will accept payment—or who have already accepted payment—from those consumers.

8. TaskUs Inc., is an U.S. outsourcing company that handles content moderation for companies including Shopify, Facebook and Doordash. See https://www.taskus.com/industries/retail-ecommerce. This is a class action for damages against TaskUs and Shopify for their failure to exercise reasonable care in securing and safeguarding consumer information in connection with a massive data breach impacting Plaintiff and the class. Shopify and TaskUs failed to have the correct "computer safeguards and access controls in place"

II. PARTIES

A. Plaintiff

9. Plaintiff **My Choice Software LLC** is, and was at all relevant times, a California Limited Liability Company with its principal place of business in Orange County, California.

B. Defendants

10. Plaintiff is informed and believes and based upon that information and belief alleges that Defendant **Shopify Inc.** is a Canadian company headquartered in Ottawa, Canada with a domestic office in San Francisco, California. Further, Shopify Inc. does business throughout the United States and in California,

including San Francisco County. Accordingly, Shopify, Inc. is a Canadian e-commerce platform that does business throughout California and the United States. See https://corporateofficeheadquarters.org/shopify/.

11. Plaintiff is informed and believes and based upon that information and belief alleges that Defendant **Shopify (USA) Inc.** is a Canadian company headquartered in Ottawa, Canada with a domestic office in San Francisco, California. Further, Shopify (USA) Inc. does business throughout the United States and in California, including San Francisco County. Accordingly, Shopify (USA) Inc. is a Canadian e-commerce platform that does business throughout California and the United States. See https://corporateofficeheadquarters.org/shopify/.

12. **Shopify Inc.** and **Shopify (USA) Inc.** are referred to collectively herein as "**Shopify**."

13. Plaintiff is informed and believes, and based upon that information and belief alleges that Defendant **TaskUs Inc**., is a Delaware Corporation headquartered in New Braunfels, Texas, and with significant contacts in California, including San Francisco County. Accordingly, Taskus, Inc. is a U.S. outsourcing company that does business throughout California and the United States. See https://www.taskus.com/locations/united-states/.

14. The true names and capacities, whether individual, corporate, associate, or otherwise, of Defendants sued herein as DOES 1 to 100, inclusive, are currently unknown to Plaintiff, who therefore sues Defendants by such fictitious names under California Code of Civil Procedure § 474. Plaintiff is informed and believes, and based thereon alleges, that each of the Defendants designated herein as a DOE is legally responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of the Defendants designated hereinafter as DOES when such identities become known.

15. Plaintiff is informed and believes, and based thereon alleges, that each Defendant acted in all respects pertinent to this action, Defendants acts as agents, employees, supervisors, partners, conspirators, servants and/or joint venturers of each other, and in doing the acts hereafter alleged, were acting within the scope and authority of such agency, employment, partnership, conspiracy, enterprise and/or joint venture, and with the express and/or implied permission, knowledge, consent, authorization and ratification of their co-defendants.

III. JURISDICTION AND VENUE

16. This Court has jurisdiction over this matter pursuant to the California Constitution, Article VI, § 10 and California Code of Civil Procedure §410.10, because Defendants transacted business and committed the acts alleged in California. More than two-thirds of the Class Members are citizens and residents of California, the Defendants are located in California, and Defendants have their principal places of business in and are headquartered in California; thus, this case is not subject to removal under the Class Action Fairness Act of 2005 under both the "home state exception" and the "local controversy exception." 28 U.S.C. § 1332(d)(4)(A) (home state exception); 28 U.S.C. § 1332 (D)(4)(B) (local controversy exception).

17. The injuries, damages and/or harm upon which this action is based occurred or arose out of activities engaged in by Shopify within, affecting, and emanating from the State of California. Shopify regularly conducts and/or solicits business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from products provided to persons in the State of California. Shopify has engaged, and continues to engage, in substantial and continuous business practices in the State of California.

18. Venue is appropriate in San Francisco County because Defendants did and are doing business in San Francisco County, and the claims arose here, and because a substantial part of the events or omissions giving rise to the claims occurred in San Francisco County.

19. Plaintiff accordingly alleges that jurisdiction and venue are proper in this Court.

V. FACTUAL BACKGROUND

A. Shopify and its Promise to Customers

20. Shopify is an e-commerce platform that enables merchants to sell products online. In **June 2019**, Shopify reported that it had more than 1,000,000 businesses in approximately 175 countries using its platform, with total gross merchandise volume exceeding $41 billion for calendar year 2018. Using Shopify's website, merchants provide Shopify with their product offerings, prices, shipping options and other business preferences. Shopify hosts some of its merchants' websites and creates all of the code necessary to implement the product catalog and to accept payment. In addition, merchants who already own websites can elect to embed certain Shopify assets, such as payment forms, into their pre-existing websites.

Regardless of the implementation, Shopify handles the collection and validation of the consumer's payment information, as well as processing the payment, through its relationships with third parties, such as Stripe.

21. To display payment forms to consumers, Shopify sends executable javascript code to consumers' computers or mobile devices, which then execute the code. Upon execution, the code loads and displays the payment forms to consumers.

22. Shopify does not disclose to consumers its role in the transaction, let alone that Shopify is sending code to consumers' devices to display the payment forms. To the consumer, the website and payment forms appear to be generated by the merchant itself. Thus, a consumer never knows that they have shared their sensitive information, including sensitive financial information, to Shopify, nor does the consumer consent to such actions.

23. For example, consumers who order apparel or accessories on the IABMFG website are presented with a cart page before proceeding to the checkout page. The bottom of the cart page features a number of icons for various forms of payment, including Visa, Mastercard and American Express. The Shopify icon is presented alongside the credit card icons, making it appear to consumers that Shopify is optional or a type of payment method the consumer could choose akin to a credit card even though it is not.

24. Consumers who proceed with purchasing goods on the IABMFG website are presented with the a payment form where there is no mention of Shopify. All of the input elements in the form (i.e., those corresponding to "Email," "First name," "Last name," "Address," "Apartment, suite, etc.," "City," "Country/Region," "State," "ZIP code," and "Phone") are generated by Shopify. To the user, however, it appears that the form and input elements are generated and provided by IABMFG. Shopify does not cause its involvement in the transaction to be displayed to the consumer alongside the payment form.

25. Only a person with technical knowledge and special software tools could determine that the payment forms are generated by Shopify. After submitting the shipping information form on the IABMFG website, the user is presented with a payment form where again there is no mention of Shopify: Once again, the payment form—including the input elements—is generated by Shopify and sent to the user's browser. To the user, however, it appears that the payment form is being generated by the IABMFG website. As is true of the shipping form, Shopify does not disclose its involvement in the transaction to the consumer.

26. When a consumer completes and submits the shipping and payment forms, it appears to the consumer that the information in the forms will be sent directly to the merchant. However, Shopify's software code, which has been installed on the user's computer without his or her consent, ensures that consumers' communications—including the private information in the forms—are intercepted and rerouted to Shopify.

27. Shopify's involvement with the consumer's private information does not end when the transaction is completed. To the contrary, Shopify's involvement has only begun. Now that Shopify has the consumer's information, Shopify will track the consumer's behavior across its vast merchant network. To achieve this, Shopify installs a tracking cookie on the user's browser. This cookie may be installed when the user visits the payment page, or any other page of the merchant's website.

28. This information is stored either by Shopify and/or by Stripe after the information is provided to it by Shopify. Shopify and/or Stripe make all of this information available to its merchants who are involved in transactions with the consumer in question. To retrieve the information, a merchant can click a button entitled "View customer data" in the Shopify user interface, and Shopify will email the data corresponding to the transactions with the merchant and consumer.

B. The Data Breach

29. Despite these promises, assurances, and representations, Shopify's document storage solutions were anything but secure. On **September 18, 2020**, My Choice Software received an email from Loren Paddelford, advising of a breach involving **423,179** total compromised merchant records from over 100 merchants.[1] The files breached included the digital software codes or "product keys" purchased and inventoried by My Choice Software, amounting to approximately **$132,870,543.50**.

30. Following public reports of the Data Breach, Shopify finally took action and provided a public statement on **September 23, 2020,** which "two 'rogue members' of its support team stole customer data from at least 100 merchants."[2]

---

[1] Zack Whitaker, "Shopify says two support staff stole customer data from sellers," https://techcrunch.com/2020/09/23/shopify-data-merchant-breach/ (Last visited September 16, 2022)

[2] *Id.*

31. On **October 19, 2020**, My Choice Software received an email from Kelly Gartshore in response to an email sent by My Choice Software prior emails requesting reasoning for the breach. Gartshore explained that the breach included access to an event log indicated an unknown person(s) installed a "private application" on My Choice Software's protected computer and network (Shopify Plus store). This incident occurred on July 16, 2020 at 15:23:59 UTC. Approximately 4 minutes later, a command was issued to export all of My Choice Software's customer and order reports (423179 out of 423179). Three hours later at 19:56:38 UTC, this "private application" was uninstalled and removed from My Choice Software's protected computer and network.

32. On **November 23, 2020**, Nate Mumme sent an email to Kelly Gartshore requesting a copy of the malicious application unlawfully installed on his protected computer and network. On **November 24, 2020**, Kelly Gartshore provided responded to Mr. Mumme and provided him with a template notice for him to consider sending to his customers about the data breach. Gartshore reiterated no full credit card numbers were compromised.

33. On **March 18, 2021**, Shopify Plus Legal emailed My Choice Software to confirm that it finished conducting its internal investigation, and briefly indicated that a dark web vendor was offering merchant data purportedly belonging to My Choice Software. Outside counsel was unable to confirm the legitimacy of the offer and found no further evidence of My Choice Software's data being available for sale because the investigation was still open with law enforcement.

34. On **March 19, 2021**, My Choice Software requested more information, including but not limited to a screen shot of the listing and or the dark web URL address of the sale. That same day, Katherine Metcalfe from Shopify providing a secure PDF containing the screenshot of the dark web sale, but did not provide the URL address.

35. On **April 19, 2021**, Katherine Metcalfe notified My Choice Software that he would be contacted after KIVU Consulting conducted its investigation.[3] As of the filing of Plaintiff's Complaint, Shopify has not disclosed the location of My Choice Software's product keys on the dark web.

[3] https://kivuconsulting.com/

36. While it is unclear when the Data Breach first began, the statement and communications with Loren Paddelford demonstrate that Shopify should have known that its database was vulnerable and sensitive information of customers and vendors could be accessed and corrupted with ease.

37. Based on information and belief, Plaintiff alleges that to date, Shopify has yet to provide a reasoning for the Data Breach to Plaintiff or all of the Class Members, that Defendant Taskus is directly responsible for the breach, and all Defendants have failed to provide the locations of the stolen inventory despite reportedly having the URL addresses of the breached data.

C. The Value of PII

38. Personal Identifiable Information ("PII") is information that can be used to distinguish, identify, or trace an individual's identity, such as their name, social security number, and biometric records. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

39. The types of information compromised in the Data Breach are highly valuable to cybercriminals. Bank account numbers, social security numbers, financial and tax records, and images of driver's licenses can all be used to defraud Shopify customers of money and property.

40. Given the nature of the Data Breach, it is foreseeable that the compromised PII could be used to access Plaintiff's and the other Class Members' financial accounts, thereby providing access to additional PII or personal and sensitive information.

41. Identity thieves can also use the PII to harm Plaintiff and the other Class Members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for

> example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[4]

42. To put it into context, the 2013 Norton report – based on one of the largest consumer cybercrime studies ever conducted – estimated that the global price tag of cybercrime was around $113 billion at that time, with the average cost per victim being $298 dollars.[5] That number no doubt increased after the PII of Plaintiff and the other Class Members was leaked in the Data Breach.

43. The problems associated with identity theft are exacerbated by the fact that many cybercriminals will wait years before attempting to use the PII they have obtained. Indeed, in order to protect themselves, Plaintiff and the other Class Members will need to remain vigilant against unauthorized data use for years and decades to come.

44. Once stolen, PII can be used in a number of different ways. One of the most common ways is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool) which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items

[4] The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, Federal Trade Commission, (April 2007), available at http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theftstrategic-plan/strategicplan.pdf (last visited April 20, 2020).

[5] Norton by Symantec, 2013 Norton Report, available at https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf (last visited April 20, 2020).

such as weapons, drugs, and PII.[6] Websites appear and disappear quickly, making it a very dynamic environment.

45. Due to its concealed and sometimes disguised nature, coupled with the intentional use of special applications to maintain anonymity, the dark web is a haven for a plethora of illicit activity, including the trafficking of stolen PII captured via data breaches or hacks.[7] One 2018 study found that an individual's online identity is worth as much as approximately $1,170 on the dark web.[8]

46. Once someone buys PII, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

47. PII can also be used by cybercriminals to target victims using phishing scams. [9]Phishing is when scammers use personal information they have obtained about victims to send fraudulent emails, texts, or copycat websites to get victims to share additional valuable personal information – such as login IDs and passwords.[10] Scammers also use phishing emails to get access to a victim's compute or network, then install programs like ransomware that can lock a victim out of important files on their computer.[11] According to one Federal Bureau of Investigation study, scammers collected more than $676 million in 2017 alone through two types of phishing scams: "Business Email Compromise" and "Email Account Compromise."[12]

---

[6] Brian Hamrick, The dark web: A trip into the underbelly of the internet, available at https://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbellyof-the-internet/8698419 (last visited April 20, 2020).

[7] Ellen Sirull, What is the Dark Web?, Experian, Apr. 8, 2018, https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/; see also The dark web: A trip into the underbelly of the internet, supra. fn. 34.

[8] Simon Migliano, Dark Web Market Place Index (US Edition), TOP10VPN, Feb. 28, 2018, https://www.top10vpn.com/privacycentral/privacy/dark-web-market-price-index-feb-2018-us/ (last visited April 20, 2020).

[9] How to Recognize and Avoid Phishing Scams, U.S. Federal Trade Commission, May 2019, https://www.consumer.ftc.gov/articles/how-recognizeand-avoid-phishing-scams (last visited April 20, 2020).

[10] *Id.*

[11] *Id.*

[12] 2017 Internet Crime Report, U.S. Federal Bureau of Investigation, https://pdf.ic3.gov/2017_IC3Report.pdf (last visited April 20, 2020).

48. The Data Breach and exposure of the PII has immediately, directly and substantially increased Plaintiff's and the other Class members' risk of identity theft. As a result of the Data Breach, Plaintiff and the other Class members have also suffered nuisance and a loss of privacy, and must now expend additional time and money mitigating the threat of identity theft, which would not have been necessary but for the Data Breach.

49. The insufficient security policies and procedures implemented by Shopify are a material fact that a reasonable consumer would take into consideration when deciding whether to provide Defendants with personal and confidential information. Had Plaintiff and the other Class Members known that Defendants failed to employ necessary and adequate protection of their PII, they would not have used Shopify or would have otherwise limited the PII shared with Defendants.

VI. CLASS ALLEGATIONS

50. Plaintiff also brings this action on behalf of himself and all others similarly situated as a class action pursuant to Code of Civil Procedure § 382. Plaintiff seeks to represent a Class composed of and defined as:

> **The Class: All persons, including natural persons and entities, in California who submitted payment information via Shopify's software between September 16, 2019 to the present.**

51. This action has been brought and may properly be maintained as a class action against Shopify because there is a well-defined community of interest in the litigation and the proposed class is easily ascertainable.

52. Plaintiff reserves the right under Rule 1855(b) of the California Rules of Court, to amend or modify the class descriptions with greater specificity or to provide further division into subclasses or limitation to particular issues.

53. This action has been brought and may properly be maintained as a class action under the provisions of the California Code of Civil Procedure § 382 because there is a well-defined community of interest in the litigation and the proposed Classes are easily ascertainable.

///

///

A. Numerosity

54. Plaintiff does not know the exact size of the Class, but he estimates that the Class is composed of more than 5,000 persons. The persons in the Class are so numerous that the joinder of all such persons is impracticable and the disposition of their claims in a class action rather than in individual actions will benefit the parties and the courts.

B. Commonality

55. This action involves common questions of law and fact to the potential Class because each class member's claim derives from the same unlawful practices of Shopify. The common questions of law and fact predominate over individual questions, as proof of a common or single set of facts will establish the right of each member of the Class to recover. The questions of law and fact common to the Class include, but are not limited to, whether Shopify has violated Sections 631 and 635 of the California Invasion of Privacy Act; whether Shopify invaded the Class members' privacy rights in violation of the California Constitution; whether Shopify violated the California Computer Data Access and Fraud Act; whether Shopify violated California's Unfair Competition Law; and whether the Class members are entitled to actual damages, statutory damages, and/or equitable relief for these violations. There are common answers to these questions which further demonstrate that class treatment is appropriate in this case.

C. Typicality

56. Plaintiff's claims are typical of the claims of other Class members because, among other things, all such claims arise out of the same unlawful course of conduct in which Shopify engaged. Plaintiff and those similarly situated used Shopify payment forms and had their electronic communications intercepted and disclosed to Shopify through the use of Shopify's wiretaps.

D. Adequacy of Representation

57. Plaintiff will fairly and adequately protect the interests of all class members because it is in his best interests to prosecute the claims alleged herein to obtain full compensation due to him for the unfair and illegal conduct of which he complains. Plaintiff also has no interests that are in conflict with, or antagonistic to, the interests of Class members. Plaintiff has retained highly competent and experienced class action attorneys to represent his interests and those of the Class. By prevailing on his own claims, Plaintiff will establish Shopify's liability to all Class members. Plaintiff and his counsel have the necessary financial

resources to adequately and vigorously litigate this class action, and Plaintiff and counsel are aware of their fiduciary responsibilities to the class members and are determined to diligently discharge those duties by vigorously seeking the maximum possible recovery for class members.

58. Plaintiff will fairly and adequately represent and protect the interests of the members of each Class. Counsel who represent Plaintiff are competent and highly experienced in litigating large class action lawsuits on a regular basis. See www.quintlaw.com.

E. Superiority of Class Action

59. A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder of all Class Members is not practicable, and questions of law and fact common to each Class predominate over any questions affecting only individual members of the Class. Each member of the Class has been damaged and is entitled to recovery by reason of Defendants' unlawful policies and practices alleged in the Complaint.

60. Class action treatment will allow those similarly situated persons to litigate their claims in the manner that is most efficient and economical for the parties and the judicial system. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

61. Class Plaintiff contemplates the eventual issuance of notice to the proposed Class Members of each Plaintiff Classes that would set forth the subject and nature of the instant action. The Defendants' own business records can be utilized for assistance in the preparation and issuance of the contemplated notices. To the extent that any further notice is required additional media and/or mailings can be used.

FIRST CAUSE OF ACTION

NEGLIGENCE

(Against All Defendants)

62. Plaintiff hereby repeats, realleges, and incorporates by reference each and every allegation contained above as though the same were fully set forth herein.

63. Plaintiff brings this cause of action individually and on behalf of the Class.

64. Defendants owed a duty to Plaintiff and the other Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in Defendants'

possession from being compromised, lost, stolen, accessed, misused, and/or disclosed to unauthorized parties. More specifically, this duty included, inter alia, (a) designing, maintaining, and testing Defendants' security systems to ensure that the PII of Plaintiff and the other Class Members in Defendants' possession was adequately secured and protected, including using encryption technologies; (b) implementing processes that would detect a breach of their security systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by Defendants' own security systems, regarding intrusions to their networks; and (d) maintaining data security measures consistent with industry standards.

65. Defendants knew or should have known that the PII of Plaintiff and the other Class Members included personal and sensitive information that is valuable to identity thieves and other criminals. Defendants also knew or should have known of the serious harms that could happen if the PII of Plaintiff and the other Class Members was wrongfully exposed, that exposure was not fixed, and/or Plaintiff and the other Class Members were not told about the exposure in a timely manner.

66. By entrusting Defendants to safeguard their PII, Plaintiff and the other Class Members had a special relationship with Defendants. Plaintiff and the other Class Members applied for Defendants' services and agreed to provide their PII with the understanding that Defendants would take appropriate measures to protect it, and would inform Plaintiff and the other Class Members of any breaches or other security concerns that might call for action by them. But Defendants did not. Defendants not only knew that their data security was inadequate, they also knew they did not have the tools to detect and document intrusions or exfiltration of PII. Defendants are morally culpable, given their knowledge of cyberattacks on the real estate industry, wholly inadequate safeguards, and refusal to notify Plaintiffs and the other Class members of breaches or security vulnerabilities.

67. Defendants owed a duty of care to Plaintiff and the other Class Members because they were foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiff and the other Class Members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendants knew that it was more likely than not Plaintiff and the other Class Members would be harmed. Defendants solicited, gathered, and stored PII provided by Plaintiff and the other Class Members in the regular

course of business. Since Defendants knew that a breach of their systems would cause damages to Plaintiff and the other Class Members, Defendants had a duty to adequately protect such sensitive personal information.

68. Defendants' duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such Shopify. Various FTC publications and data security breach orders further form the basis of Shopify's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

69. Defendants also had a duty to safeguard the PII of Plaintiff and the other Class Members and to promptly notify them of a breach based on state laws and statutes that require Defendants to reasonably safeguard PII, as detailed herein.

70. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class Members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite repeated failures and intrusions, and allowing unauthorized access to their PII.

71. Defendants' failure to comply with industry and federal regulations further evidences their negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class Members' PII.

72. Defendants' breaches of these duties were not merely isolated incidents or small mishaps. Rather, the breaches of the duties set forth above resulted from a long-term company-wide refusal by Defendants to acknowledge and correct serious and ongoing data security problems.

73. Defendants also owed a duty to Plaintiff and the other Class Members to timely disclose any incidents of data breaches, where such breaches compromised the PII of Plaintiff and the other Class Members. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiff and the other Class Members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit

reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Defendants' misconduct. Plaintiff and the other Class Members were foreseeable and probable victims of any inadequate notice practices. Defendants knew that, through their actions and omissions, they had caused the sensitive PII of Plaintiff and the other Class Members to be compromised and accessed by unauthorized persons yet failed to mitigate potential harm to their customers by providing timely notice of the Data Breach.

74. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and the other Class Members, their PII would not have been compromised, stolen, accessed and/or viewed by unauthorized persons.

75. As a direct, proximate and legal result of Defendants' negligence, Plaintiff and the other Class Members have been injured as described herein, and are entitled to damages in an amount to be proven at trial. Plaintiff and the other Class Members' injuries include, but are not limited to, the following:

a. purchasing goods and services they would not have otherwise paid for and/or paying more for good and services than they otherwise would have paid, had they known the truth about Defendants' substandard data security practices;

b. losing the inherent value of their PII;

c. losing the value of the explicit and implicit promises of data security;

d. identity theft and fraud resulting from the theft of their PII;

e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

g. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including

missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

j. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

76. The injury and harm suffered by Plaintiff and the other Class Members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class Members' PII. Defendants knew their systems and technologies for processing and securing the PII of Plaintiffs and the other Class members had numerous security vulnerabilities.

77. As a result of this misconduct by Defendants, the PII of Plaintiff and the other Class Members was compromised, placing them at a greater risk of identity theft or subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiff and the other Class Members also suffered diminution in value of their PII in that it is now easily available to hackers on the dark web. In addition, Plaintiff and the other Class Members have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

78. Defendants' misconduct as alleged herein constitutes malice or oppression in that it was despicable conduct carried on by Defendants with a willful and conscious disregard of the rights or safety of Plaintiff and the other Class Members and that despicable conduct has subjected Plaintiff and the other Class Members to cruel and unjust hardship in conscious disregard of their rights. As a result,

Plaintiff and the other Class Members are entitled to injunctive relief, as well as, actual and punitive damages against Defendants.

SECOND CAUSE OF ACTION

BREACH OF CONTRACT

(Against All Shopify Defendants)

79. Plaintiff and the Members of the Class re-allege and incorporate by reference, as though fully set forth herein, the paragraphs previously alleged in this Complaint.

80. This claim is brought by Plaintiff, on behalf of the Class and the subclasses thereof.

81. Plaintiffs and the other Class members entered into a contract with Shopify for the provision of title insurance, a home warranty, or other closing services.

82. The terms of Shopify's Privacy Policy are part of the contract.

83. Shopify's Privacy Policy is an agreement between Shopify and individuals who provided their PII to Shopify, including Plaintiff and other Class Members, even after they are no longer a customer of Shopify.

84. Shopify's Privacy Policy "governs [Shopify's] use of the information [customers] provide us," and applies when Shopify receives information (1) from individuals "on applications, forms and in other communications to [Shopify], whether in writing, in person, by telephone or any other means"; (2) about individuals' "transactions with [Shopify, its] affiliated companies, or others"; and (3) about individuals "from a consumer reporting agency."

85. Plaintiff and the other Class Members provided their PII to Defendants when they, among other things, applied for and/or purchased title insurance, a home warranty, and/or other real estate transaction closing services provided by Defendants.

86. Plaintiff and the other Class Members performed substantially all that was required of them under their contract with Shopify, or they were excused from doing so.

87. Plaintiff and the other Class Members performed substantially all that was required of them under their contract with Shopify, or they were excused from doing so. Conversely, Shopify, in collecting Plaintiff's and the other Class Members' PII, manifested its intent to adhere to its obligations

under the Privacy Policy, including using its "best efforts to ensure that no unauthorized parties have access to any of [its customers'] information."

88. Further, Shopify stated that it "currently maintain[s] physical, electronic, and procedural safeguards that comply with federal regulations to guard [customers'] nonpublic personal information.

89. Shopify failed to perform its obligations under the contract, including failing to provide adequate privacy, security, and confidentiality safeguards for Plaintiff's and the other Class Members' information and documents.

90. As a direct and proximate result of Shopify's breach of contract, Plaintiff and the other Class Members did not receive the full benefit of the bargain, and instead received title insurance, a home warranty, and/or other closing services that were less valuable than described in their contracts. Plaintiff and the other Class Members, therefore, were damaged in an amount at least equal to the difference in value between that which was promised and Defendants' deficient performance.

91. As an additional direct and proximate result of Defendants' breach of contract, Plaintiff and the other Class Members have suffered actual damages resulting from the exposure of their PII information, and they remain at imminent risk of suffering additional damages in the future.

92. Accordingly, because Plaintiff and the other Class Members have been injured by Defendants' breach of contract, they are entitled to damages and/or restitution in an amount to be proven at trial.

THIRD CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

(Against All Shopify Defendants)

93. Plaintiff and the Members of the Class re-allege and incorporate by reference, as though fully set forth herein, the paragraphs previously alleged in this Complaint.

94. Defendants solicited and invited Plaintiff and the other Class Members to apply for their services. Plaintiff and the other Class Members accepted Defendants' offer and provided documents containing PII to Defendants, and if approved, money, in exchange for Defendants' title insurance, home warranty and/or other real estate transaction closing services.

95. When Plaintiff and the other Class Members applied for Shopify's services and products, they provided their PII. In so doing, Plaintiff and the other Class Members entered into implied contracts with Shopify pursuant to which it agreed to safeguard and protect their PII and to timely and accurately notify them if their PII was breached or compromised.

96. Each application for Shopify's service or product made by Plaintiff and the other Class Members was made pursuant to the mutually agreed upon implied contract with Shopify under which it agreed to safeguard and protect their PII.

97. Plaintiff and the other Class Members entered into the implied contracts with the reasonable expectation that Shopify's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and the other Class members believed that Shopify would use part of the monies paid to Shopify under the implied contracts to fund adequate and reasonable data security practices.

98. Plaintiff and the other Class Members would not have provided and entrusted their PII to Shopify or would have paid less for Shopify's services in the absence of the implied contract or implied terms between them and Shopify. The safeguarding of the PII of Plaintiff and the other Class Members and prompt and sufficient notification of a breach was critical to realize the intent of the parties.

99. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Shopify.

100. Shopify breached its implied contracts with Plaintiff and the other Class Members to safeguard and protect their PII when it (a) failed to have security protocols and measures in place to protect that information; (b) disclosed that information to unauthorized third parties; and (c) failed to provide timely and accurate notice that their PII was compromised as a result of the Data Breach.

101. As a direct and proximate result of Shopify's breaches of the implied contracts between it and Plaintiff and the other Class Members, Plaintiff and the other Class Members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid.

///

FOURTH CAUSE OF ACTION

BREACH OF CONFIDENCE

(Against All Defendants)

102. Plaintiff and the Members of the Class re-allege and incorporate by reference, as though fully set forth herein, the paragraphs previously alleged in this Complaint.

103. This claim is brought by Plaintiff on his behalf, and on behalf of Class Members and the subclasses thereof.

104. This claim is asserted against Defendants for breach of confidence concerning the PII that Plaintiff and the other Class members provided to Defendants in confidence.

105. At all times during Plaintiff's and the other Class Members' interactions with Defendants, Defendants were fully aware of the confidential nature of the PII that Plaintiff and the other Class Members shared with Defendants.

106. Plaintiff and the other Class Members reasonably expected that their PII would be collected, stored, and protected in confidence by Defendants, and not disclosed to unauthorized third parties. Plaintiff and the other Class Members provided their respective PII to Defendants with the understanding that Defendants would protect and not permit that PII to be disseminated to any unauthorized third parties.

107. Defendants voluntarily received in confidence Plaintiff's and the other Class Members' PII with the understanding that that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

108. On information and belief, due to Defendants' failure to prevent, detect, and stop the Data Breach from occurring, Plaintiff's and the other Class Members' PII was disclosed and misappropriated to unauthorized malicious third parties beyond their confidence and without their express permission.

109. Defendants' Privacy Policy contained an implied obligation on behalf of Defendants to promptly inform Plaintiff and the other Class Members of any breach by Defendants of their Privacy Policy and to take appropriate remedial measures to protect Plaintiff's PII. This implied obligation is consistent with industry standards and practices related to large data breaches.

110. Following Defendants' failure to prevent, detect, and stop the Data Breach from occurring, Defendants failed to promptly inform Plaintiff and the other Class Members that their PII was disclosed, the

extent of the breach, and any remedial measures Defendants have taken to remediate the breach or protect the misappropriated PII.

111. As a direct and proximate cause of Defendants' actions and inactions, Plaintiff and the other Class Members have suffered injury and damages.

112. But for Defendants' exposure of PII in violation of the parties' understanding that it would be held in confidence, Plaintiff's and the other Class Members' PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' exposure was a direct and legal cause of the theft of Plaintiff's and the other Class Members' PII, as well as their resulting damages.

113. The injury and harm Plaintiff and the other Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized exposure of Plaintiff's and the other Class Members' PII. On information and belief, Defendants knew their computer systems and technologies for accepting and securing Plaintiff's and the other Class Members' PII had numerous security vulnerabilities, but Defendants continued to collect, store, and maintain Plaintiff's and the other Class Members' PII without fixing the vulnerabilities.

114. On information and belief, because of Defendants' misconduct, Plaintiff's and the other Class Members' PII was compromised – placing them at a greater risk of identity theft and subjecting them to identity theft and fraud – and disclosed to unauthorized, malicious, third parties without their consent. Plaintiff and the other Class Members also suffered diminution in value of their PII in that it became easily available to hackers on the dark web. Plaintiff and the other Class Members have also suffered consequential out-of-pocket losses for procuring credit freezes or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

FIFTH CAUSE OF ACTION

FOR UNLAWFUL COMPETITION AND UNLAWFUL BUSINESS PRACTICES

[CALIFORNIA BUSINESS & PROFESSIONS CODE §§ 17200, et seq.]

(Against All Defendants)

115. Plaintiff and the Members of the Class re-allege and incorporate by reference the paragraphs previously alleged in this Complaint.

116. On information and belief, because of Defendants' misconduct, Plaintiff's and the other

Class Members' PII was compromised – placing them at a greater risk of identity theft and subjecting them to identity theft and fraud – and disclosed to unauthorized, malicious, third parties without their consent. Plaintiff and the other Class Members also suffered diminution in value of their PII in that it became easily available to hackers on the dark web. Plaintiff and the other Class Members have also suffered consequential out-of-pocket losses for procuring credit freezes or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

117. Defendants are "persons" as defined by California Business & Professions Code § 17201.

118. Defendants violated Business & Professions Code § 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

119. Business & Professions Code § 17200 prohibits acts of "unfair competition," including any "unlawful, unfair or fraudulent business act or practice" and "unfair, deceptive, untrue or misleading advertising."

120. Defendants' "unfair" acts and practices – all of which are immoral, unethical, oppressive, unscrupulous and/or substantially injurious to consumers – include:

a. Failing to implement and maintain reasonable security measures to protect Plaintiff's and the other Class Members' PII from unauthorized exposure, disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Further, Shopify failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following the identification of security risks. This conduct with little if any utility, is unfair when weighed against the harm to Plaintiff and the other Class Members, whose PII has been compromised.

b. Failing to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, and California's Consumer Records Act, Civil Code § 1798.81.5.

c. Failing to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing

benefits to consumers or competition. Moreover, because consumers could not know of Defendants' inadequate security, consumers could not have reasonably avoided the harms that Defendants caused.

d. Engaging in unlawful business practices by violating Civil Code § 1798.82.

121. Defendants have engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Civil Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Civil Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and California common law.

122. Defendants' unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the other Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following identified risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. §45, and California's Customer Records Act, Civil Code §§ 1798.80, et seq., which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Civil Code §§ 1798.80, et seq.;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and the other Class members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common

law and statutory duties pertaining to the security and privacy of Plaintiff and the other Class members' PI, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Civil Code § 1798.80, et seq.

123. Plaintiff and the other Class Members are reasonable consumers who expected Defendants to protect vigorously their Personal Information entrusted to Defendants and to be informed by Defendants of potential and actual cybersecurity vulnerabilities as soon as Defendants became aware of such threats.

124. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' personal information.

125. Defendants' acts and omissions were intended to induce Plaintiff and the other Class Members' reliance on Defendants' promise that their PII was secure and protected and/or their failure to disclose otherwise, to increase the number of Class Members, and, ultimately, to increase Defendants' revenues. Plaintiff and the other Class Members were deceived by Defendants' failure to properly implement adequate, commercially reasonable security measures to protect their PII, and Defendants' failure to promptly notify them of the security breach. As a result, Defendants' conduct constitutes "fraudulent" business acts or practices.

126. Defendants' conduct was and is likely to deceive consumers. In failing to implement adequate security procedures and protocols to protect Plaintiff's and the other Class Members' PII, and to promptly notify Plaintiff and the other Class Members of potential and actual security threats, Defendants have knowingly and intentionally concealed material facts and breached their duty not to do so.

127. Defendants were under a duty to Plaintiff and the other Class Members to protect Class Members' PII and promptly notify Class Members of potential and actual security threats, and other omitted facts alleged herein, because:

a. Defendants were in a superior position to know the specifics of a potential or actual security breach; and

b. Defendants actively concealed information known to them regarding potential and actual security breaches affecting Class Members' account information.

c. Defendants have still not provided Plaintiff and the other Class Members with a

comprehensive or detailed report on which customers were affected, and what information was stolen. Accordingly, Plaintiff and the other victims of the Data Breach do not have the information they need to take informed and appropriate actions to mitigate the damage caused by the Data Breach and to protect against future acts of cyber-fraud.

128. The facts Defendants concealed from or did not disclose to Plaintiff and the other Class Members are material in that a reasonable person would have considered them to be important in deciding whether to use Defendants' services. Had Plaintiff and other Class Members known that Defendants failed to employ necessary and adequate protection of their PII and would fail to timely notify them of potential security breaches, they would not have used Defendants' services or would have paid much less for their services.

129. By their conduct, Defendants have engaged in unfair competition and unlawful, unfair and fraudulent business practices. Defendants' unfair or deceptive acts or practices occurred repeatedly in Defendants' trade or business and were capable of deceiving a substantial portion of the purchasing public.

130. As a direct and proximate result of Defendants' unlawful, unfair and deceptive acts and practices, Plaintiff and the other Class Members suffered and will continue to suffer injury in fact. Plaintiff and the other Class Members lost money or property as a result of purchasing services from Defendants, the premiums and/or price received by Defendants for their services, the loss of the benefit of their bargain with Defendants as they would not have paid Defendants for services or would have paid less for such services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

131. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff and the other Class Members' rights. Past data breaches within the industry put it on notice that its security and privacy protections were inadequate.

132. Defendants have been unjustly enriched and should be required to make restitution to Plaintiff and the other Class Members pursuant to Business & Professions Code §§ 17203 and 17204. Pursuant to Business & Professions Code § 17203, Plaintiff and the Class Members seek an order of this Court enjoining Defendants from continuing to engage in unlawful, unfair, and fraudulent business practices

and any other act prohibited by law, including those set forth in this Complaint.

133. Plaintiff and the other Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under Code of Civil Procedure § 1021.5; injunctive relief enjoining Defendants from continuing to employ deficient data security pursuant to California Business and Professions Code § 17203; and other appropriate equitable relief.

SIXTH CAUSE OF ACTION

VIOLATION OF CALIFORNIA CONSUMERS LEGAL REMEDIES ACT

[CALIFORNIA CIVIL CODE § 1750, *et seq.*]

(Against All Defendants)

134. Plaintiff and the Members of the Class re-allege and incorporate by reference, as though fully set forth herein, the paragraphs previously alleged in this Complaint.

135. Plaintiff and the other Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under Code of Civil Procedure § 1021.5; injunctive relief enjoining Defendants from continuing to employ deficient data security pursuant to Business & Professions Code § 17203; and other appropriate equitable relief.

136. The Consumers Legal Remedies Act, Civil Code § 1750, et seq. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to serve its underlying purpose: Protecting consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

137. Defendants are "persons" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

138. Civil Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

///

139. In addition, Civil Code § 1770(a)(7) prohibits one who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another."

140. Plaintiffs and the other Class members are "consumers," as defined by Civil Code §§ 1761(d) and 1770, and have engaged in "transactions" with Defendants, as defined by Civil Code §§ 1761(e) and 1770.

141. Defendants acts and practices were intended to and did result in the sales of products and services to Plaintiff and the other Class Members in violation of Civil Code § 1770, including, but not limited to, the following:

a. Representing that services have characteristics that they do not have;

b. Representing that services are of a particular standard, quality, or grade when they were not;

c. Advertising services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

142. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

143. Had Defendants disclosed to Plaintiff and the other Class Members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and the other Class Members' PII as part of the services Defendants provided and for which Plaintiff and the other Class Members paid without being advised that Defendants' data security practices were insufficient to maintain the safety and confidentiality of their PII. Accordingly, Plaintiff and the other Class Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

144. By misrepresenting that they took appropriate measures to protect Plaintiff and the other Class Members' PII, Defendants violated Civil Code § 1770.

145. Defendants' acts and omissions were intended to induce Plaintiff and the other Class Members' reliance on Defendants' promise that their PII was secure and protected and/or Defendants' failure

to disclose otherwise, to increase the number of Class Members, and, ultimately, to increase Defendants' revenues. Plaintiff and the other Class Members were deceived by Defendants' failure to properly implement adequate, commercially reasonable security measures to protect their PII.

146. As a result of their reliance on Defendants' representations and omissions, Plaintiff and the other Class Members suffered an ascertainable loss due to Defendants' failure to provide adequate protection of their personal and confidential information. This loss was also the direct result of Defendants' failure to provide timely and sufficiently informative notice and warning of potential and actual cybersecurity breaches.

147. As a result of engaging in such unfair methods of competition and unfair or deceptive acts or practices, Defendants have violated Civil Code § 1770.

148. As a direct and proximate result of Defendants' violations of Civil Code § 1770, Plaintiff and the other Class Members suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for services or would have paid less for such services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing credit cards; loss of value of their PII; and/or an increased, imminent risk of fraud and identity theft. Plaintiff and the other Class Members lost money or property as a result of applying for services from Defendants.

149. Plaintiff and the other Class Members have provided notice of their claims for damages to Defendants, in compliance with Civil Code § 1782(a).

150. Plaintiff and the other Class Members seek all monetary and nonmonetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

///

///

///

///

///

SEVENTH CAUSE OF ACTION

DECEIT BY CONCEALMENT

[CALIFORNIA CIVIL CODE §§ 1709, 1710]

(Against All Defendants)

151. Plaintiff and the Members of the Class re-allege and incorporate by reference the paragraphs previously alleged in this Complaint

152. Plaintiff brings this cause of action individually and on behalf of the Class.

153. Plaintiff and the other Class Members seek all monetary and nonmonetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

154. At the time Plaintiff and the other Class Members provided their PII to Defendants, Defendants had an obligation to disclose to Plaintiff and the other Class members that their PII was an easy target for hackers and Defendants were not implementing measures to protect them.

155. Defendants failed to make the required disclosures when they requested and received Plaintiff and the other Class members' PII. Instead, Defendants willfully deceived Plaintiff and the other Class Members by concealing the true facts concerning their data security, which Defendants were obligated and had a duty to disclose, and by willfully allowing their customers to rely upon Defendants' false assurances that their PII and other data was safe and that Defendants were dedicated to maintaining that security.

156. Had Defendants disclosed the true facts about their poor data security, Plaintiff and the other Class Members would have taken measures to protect themselves or used another company for their title insurance, home warranty, and/or other real estate transaction closing services. Plaintiff and the other Class Members justifiably relied on Defendants to provide accurate and complete information about Defendants' data security, and Defendants did not. Further, independent of any representations made by Defendants, Plaintiff and the other Class Members justifiably relied on Defendants to provide title insurance, a home warranty, and/or other real estate transaction closing services with at least minimally adequate security measures and justifiably relied on Defendants to disclose facts undermining that reliance.

157. Rather than cease offering a clearly unsafe and defective services or disclosing to Plaintiff and the other Class Members that their services were unsafe and users' PII was exposed to theft on a grand scale, Defendants continued and concealed information relating to the inadequacy of their security.

158. These actions are "deceit" under Civil Code § 1710 in that they are the suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.

159. As a result of this deceit by Defendants, they are liable under Civil Code § 1709 for "any damage which [Plaintiff and the Class] thereby suffer[]."

160. Because of this deceit by Defendants, the PII of Plaintiff and the other Class Members was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiff and the other Class Members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiff and/or the other Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and/or other expenses relating to identity theft losses or protective measures.

161. Defendants' deceit as alleged herein is fraud under Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants conducted with the intent on the part of Defendants of depriving Plaintiff and the other Class Members of "legal rights or otherwise causing injury." As a result, Plaintiff and the other Class Members are entitled to punitive damages against Defendants under Civil Code § 3294(a).

EIGHTH CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA CONSUMER RECORDS ACT

[CALIFORNIA CIVIL CODE §§ 1798.80, *et seq.*]

(Against All Defendants)

162. Plaintiff and the Members of the Class re-allege and incorporate by reference, as though fully set forth herein, the paragraphs previously alleged in this Complaint.

///

163. Defendants' deceit as alleged herein is fraud under Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants conducted with the intent on the part of Defendants of depriving Plaintiff and the other Class Members of "legal rights or otherwise causing injury." As a result, Plaintiffs and the other Class members are entitled to punitive damages against Defendants under Civil Code § 3294(a).

164. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted Civil Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident … implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

165. Defendants are "businesses," as defined by Civil Code § 1798.80(a), that own, maintain and license PII within the meaning of § 1798.81.5, about Plaintiff and the Class Members.

166. Businesses that own or license computerized data that includes PII are required to notify California residents when their Personal Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Civil Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Civil Code § 1798.82.

167. Defendants are businesses that own or license computerized data that includes PII as defined by Civil Code § 1798.82.

168. Plaintiff and the other Class Members are "individual[s]" as defined by Civil Code § 1798.80(d).

169. Plaintiff and the other Class Members' PII compromised, accessed and/or taken in the Data Breach includes "personal information" as defined by Civil Code §§ 1798.80(e), 1798.81.5(d) and 1798.82, which includes:

> "information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description,

> address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information."

170. The breach of Plaintiff's and the other Class Members' PII was a "breach of the security system" of Defendant as defined by Civil Code § 1798.82(g).

171. By failing to implement reasonable security measures which would appropriately secure Plaintiff's and the other Class Members' PII, Defendants violated Civil Code § 1798.81.5.

172. In addition, by failing to notify in a timely and accurate fashion all affected Class Members that their PII had been or may have been acquired by unauthorized persons in the Data Breach, Defendants violated Civil Code § 1798.82.

173. As a direct and proximate result of Defendants' violations of Civil Code §§ 1798.81.5 and 1798.82, Plaintiff and the Class Members suffered damages because they have lost the opportunity to immediately:

a. buy identity protection, monitoring, and recovery services;
b. flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service;
c. purchase or otherwise obtain credit reports, monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or medical services;
d. place and renew credit fraud alerts on a quarterly basis;
e. routinely monitor public records, loan data, or criminal records;
f. contest fraudulent charges and other forms of criminal, financial and medical identity theft, and repair damage to credit and other financial accounts; and
g. take other steps to protect themselves and recover from identity theft and fraud.

174. In addition, because of Defendants' violation of Civil Code § 1798.81.5, Plaintiff and the other Class Members have incurred and will incur damages including, but not necessarily limited to:

a. the loss of the opportunity to control how their PII is used;

b. the diminution in the value and/or use of their PII entrusted to Defendants for the purpose of deriving services from Defendants and with the understanding that Defendants would safeguard their PII against theft and not allow access and misuse of their PII by others;

c. the compromise, publication, and/or theft of their PII, out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the breach including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from identity data misuse;

e. costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets;

f. unauthorized use of compromised PII to open new financial and/or health care or medical accounts, tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected;

g. the continued risk to their PII, which remain in Defendants' possession and are subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their possession; and

h. future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the Class Members.

175. Because they violated Civil Code §§ 1798.81.5 and 1798.82, Defendants "may be enjoined" under Civil Code § 1798.84(e).

176. Plaintiff requests that the Court enter an injunction requiring Defendants to inform Class Members of the Data Breach and implement and maintain reasonable security procedures to protect Plaintiff

and the other Class Members' PII including, but not limited to, ordering that Defendants:

a. engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

b. engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices;

c. audit, test, and train their security personnel regarding any new or modified procedures;

d. conduct regular database scanning and securing checks consistent with prudent industry practices;

e. periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices;

f. receive periodic compliance audits by a third party regarding the security of the computer systems, cloud-based services, and application software Defendants use to store the PII of California Sub-Class Members;

g. meaningfully educate California Sub-Class Members about the threats they face because of the loss of their PII to third parties, as well as the steps they must take to protect themselves; and

h. provide ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and the other California Sub-Class members.

177. Plaintiff seeks all remedies available under Civil Code § 1798.84, including actual and statutory damages, equitable relief, and reasonable attorneys' fees. Plaintiff also seeks reasonable attorneys' fees and costs under applicable law including Code of Civil Procedure § 1021.5.

PRAYER

WHEREFORE, Plaintiff demands a JURY TRIAL and prays for judgment as follows:

(a) For an Order Certifying the Class and appointing Plaintiff as the Class Representatives for the Class;

(b) For an Order Appointing Quintilone & Associates as Class Counsel for the Class;

(c) Finding that Defendants' conduct was negligent, in breach of contract and implied contract, and unlawful as alleged herein;

(d) An order permanently enjoining Defendants from further unfair, unlawful, and deceptive business acts and practices described herein;

(e) Awarding Plaintiff and Class members actual, compensatory, and consequential damages;

(f) Awarding Plaintiff and Class members restitution and disgorgement;

(g) Requiring Defendants to provide appropriate credit monitoring services to Plaintiff and Class members;

(h) Awarding Plaintiff and Class members punitive damages;

(i) Awarding Plaintiffs and Class members pre-judgment and post-judgment interest;

(j) Awarding Plaintiff and Class members reasonable attorneys' fees, costs and expenses; and

(k) Granting such other relief as the Court deems just and proper.

Dated: September 16, 2022

QUINTILONE & ASSOCIATES

By: _____

RICHARD E. QUINTILONE II,
JEFFREY T. GREEN,
KYLE J. GALLEGO,
Attorneys for Plaintiff MY CHOICE SOFTWARE, LLC, individually, and on behalf of a Class of all other persons similarly situated

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial of the claims by jury to the extent authorized by law.

Dated: September 16, 2022

QUINTILONE & ASSOCIATES

By: _____

RICHARD E. QUINTILONE II,
JEFFREY T. GREEN,
KYLE J. GALLEGO,
Attorneys for Plaintiff MY CHOICE SOFTWARE, LLC individually, and on behalf of a Class of all other persons similarly situated

NOTICE TO PLAINTIFF

A Case Management Conference is set for:

DATE: **FEB 15, 2023**

TIME: **10:30 am**

PLACE: **Department 610**
400 McAllister Street
San Francisco, CA 94102-3680

All parties must appear and comply with Local Rule 3.

CRC 3.725 requires the filing and service of a case management statement form CM-110 no later than 15 days before the case management conference. However, it would facilitate the issuance of a case management order **without an appearance** at the case management conference if the case management statement is filed and served twenty-five days before the case management conference.

Plaintiff must serve a copy of this notice upon each party to this action with the summons and complaint. Proof of service subsequently filed with this court shall so state. **This case is eligible for electronic filing and service per Local Rule 2.11. For more information, please visit the Court's website at www.sfsuperiorcourt.org under Online Services.**

[DEFENDANTS: Attending the Case Management Conference does not take the place of filing a written response to the complaint. You must file a written response with the court within the time limit required by law. See Summons.]

ALTERNATIVE DISPUTE RESOLUTION REQUIREMENTS

IT IS THE POLICY OF THE SUPERIOR COURT THAT EVERY CIVIL CASE SHOULD PARTICIPATE IN MEDIATION, ARBITRATION, NEUTRAL EVALUATION, AN EARLY SETTLEMENT CONFERENCE, OR OTHER APPROPRIATE FORM OF ALTERNATIVE DISPUTE RESOLUTION PRIOR TO A TRIAL.

(SEE LOCAL RULE 4)

Plaintiff **must** serve a copy of the Alternative Dispute Resolution (ADR) Information Package on each defendant along with the complaint. (CRC 3.221.) The ADR package may be accessed at www.sfsuperiorcourt.org/divisions/civil/dispute-resolution or you may request a paper copy from the filing clerk. All counsel must discuss ADR with clients and opposing counsel and provide clients with a copy of the ADR Information Package prior to filing the Case Management Statement.

Superior Court Alternative Dispute Resolution Administrator
400 McAllister Street, Room 103-A
San Francisco, CA 94102
(415) 551-3869

See Local Rules 3.3, 6.0 C and 10 B re stipulation to judge pro tem.

SUPERIOR COURT OF CALIFORNIA

COUNTY OF SAN FRANCISCO

DEPARTMENT 304

MY CHOICE SOFTWARE, LLC, a California Limited Liability Company, individually, and on behalf of all others similarly situated,

Plaintiff,

v.

SHOPIFY, INC., a Canadian Corporation; SHOPIFY (USA) Inc., a Delaware Corporation; TASKUS INC., a Delaware Corporation; and DOES 1 through 100, inclusive,

Defendants.

Case No. CGC-22-601842

ORDER CONTINUING MARCH 7, 2023 CASE MANAGEMENT CONFERENCE

The Court has reviewed Plaintiff's Case Management Conference Statement. In light of the representations in that statement that a related action is pending in the U.S. District Court for the Central District of California and that the parties are actively working to settle both cases, the initial Case Management Conference currently scheduled for March 7, 2023 is hereby continued to June 5, 2023. At least five court days before the continued Case Management Conference, the parties shall file a **joint** case

management conference statement that addresses the issues set forth in the Court's procedures, which are attached hereto as Exhibit A.

IT IS SO ORDERED.

Dated: March 2, 2023

Ethan P. Schulman
Judge of the Superior Court

EXHIBIT A

Superior Court of California

County of San Francisco

Department 304 - Judge Ethan P. Schulman

Complex Litigation – Procedures

Department 304 Staff:

- Clerk: Ericka Larnauti
- Clerk Phone: 415-551-3729/5948
- Attorney: Kiara Canales
- Department 304 Email: complexlit@sftc.org

Communications with the Court and Reserving Hearing Dates:

- Prior to filing any motion, all motion hearing dates must be reserved with the clerk of Department 304. Parties may not file a motion without Court approval of the hearing date and time.
- Generally, the clerk of Department 304 prefers email communications. If a party emails the clerk, they must include all counsel on the email.

Continuances:

- If the parties wish to continue a motion or a CMC, the parties may (1) submit a stipulation and proposed order; or (2) email the Court (copying all parties) at least three court days prior to the scheduled matter requesting a continuance and indicating that all parties agree to the continued date/time.

Hearing Date Vacated by Party:

- If a moving party removes a motion from the Court's calendar (either on its own, or by submitting to the Court's tentative ruling on the motion), the party must notify all other parties by email or telephone.

Appearances:

- Counsel may appear for hearings in person, via Zoom, or via CourtCall. Should the parties wish to appear via Zoom, they are to jointly email the Complex Litigation Department to make that request. The request must include each attorney's name, firm, address, telephone number, and email address and the name(s) of the client(s) each is representing. Upon receipt, the clerk will send a Zoom link for the conference. The parties may not split an appearance via Zoom and CourtCall due to sound interference.

Discovery:

- The procedures outlined below apply only to parties. With regard to discovery disputes with non-parties, the interested parties may elect to participate in this procedure, but are not required to do so.
- All deadlines for filing motions to compel discovery pursuant to the Civil Discovery Act, Code of Civil Procedure section 2016.010 *et seq.*, are vacated and suspended. No party may move to compel discovery, or file any other discovery motion, until the parties have had a discovery conference with the Court.
- Counsel must have completed all meet and confer obligations before scheduling a discovery conference.
- To request a discovery conference with the Court, counsel must contact the clerk of Department 304. Once a conference is scheduled, counsel are responsible for setting up a Zoom link or telephone conference line.
- At least three court days before the conference, counsel must email a **joint** letter outlining the discovery dispute, not exceeding 5 pages, single-spaced.
- If the discovery dispute is not resolved following the conference, any party may proceed to file a motion. Any such motion must be filed within 10 court days of the conference.
- The parties are relieved of the requirement to file a separate statement in discovery motions.
- For discovery motions, the Court prefers streamlined papers in which counsel state the discovery request and response followed by a discussion of whether a further response is or is not required. In lieu of the usual discovery motion briefing, the parties may instead provide one single filing that includes the question, the response and why more information is owed or not owed. The Court is open to the parties agreeing to an expedited briefing schedule where one side files a 5-page motion, the other side files a 5-page response, the moving party a 3-page reply and a hearing date is set 10 days out from the last filing.

E-Filing:

- The e-filing vendor for the San Francisco Superior Court Complex Department is File&Serve*Xpress*. Counsel must register with and submit all filings through said vendor. Counsel must also add themselves to the vendor's e-service list. Customer Service for e-filing registration, training information, and service list assistance can be found at support@fileandservexpress.com or by calling File&Serve*Xpress* at 888-529-7587.
- All court orders will be e-served through File&Serve*Xpress*. All counsel must add their office to the service list at File&Serve*Xpress*.
- Pursuant to California Code of Civil Procedure section 1010.6, California Rules of Court, rule 2.251 *et seq.*, and San Francisco Superior Court Local Rule 2.11, all discovery requests and responses, not filed with the court, must be electronically served, unless it is not feasible to do so (e.g., drawings, charts, etc.).
- Pursuant to Code of Civil Procedure section 1010.6(b)(3), any document received electronically by the court between 12:00 a.m. and 11:59:59 p.m. on a court day shall be deemed filed that day; any document received by a court on a non-court day will be deemed filed on the next court day.

- Pursuant to Code of Civil Procedure section 1010.6(a)(5), any document served electronically between 12:00 a.m. and 11:59:59 p.m. on a court day will be deemed served that day; any document electronically served on a non-court day will be deemed served the next court day.

Courtesy Copies:

- Counsel are directed to deliver two hard copies of all e-filed documents to Department 304, which includes proposed orders.

Challenging Confidentiality Designations:

- If the parties enter into a stipulation for a protective order, the protective order must include the language found in Attachment 1 governing the process for any party to challenge the confidentiality designation.

Sealing Motions:

- Regarding motions to seal, the Court reminds counsel to follow California Rules of Court, rules 2.550-2.551. These requirements do not apply to discovery motions but do apply to all other types of motions. Please do not submit sealed documents unless the parties need the Court to consider them. Please read *Overstock.Com, Inc. v. Goldman Sachs Grp., Inc.* (2014) 231 Cal.App.4th 471. The Court is required to follow the California Rules of Court and make specific findings.
- For motions to seal (and accompanied unredacted versions of documents conditionally lodged under seal with the Court,) the parties must highlight in yellow the proposed sealing request in the unredacted documents.

Tentative Rulings:

- For most motions, tentative rulings will be emailed directly to counsel prior to the hearing.

Court Reporters:

- The Court does not provide court reporters for hearings.
- The Court recommends that the parties obtain court reporters for substantive motions.
- The Court requests that the parties arrange for the Court to be provided with hearing transcripts following substantive motions. This is not required.

CMC Statements:

- A joint case management conference statement must be filed, and two copies delivered to Department 304, no later than five court days prior to the case management conference. Individual statements will not be considered. Do not use the Judicial Council form for case management conference statements.

- The purpose of the joint statement is that it requires counsel to confer. It shows the Court that the parties have been in direct communication.
- CMC statements are not advocacy statements. They are an agenda for a discussion. CMC statements should explain where the case is, where it is going, and how it can most efficiently reach its destination.

ATTACHMENT 1

SUPERIOR COURT OF CALIFORNIA

COUNTY OF SAN FRANCISCO

COMPLEX LITIGATION

CHALLENGING CONFIDENTIALITY DESIGNATIONS

Timing of Challenges. Any Party or Non-Party may challenge a designation of confidentiality at any time. Unless a prompt challenge to a Designating Party's confidentiality designation is necessary to avoid foreseeable, substantial unfairness, unnecessary economic burdens, or a significant disruption or delay of the litigation, a Party does not waive its right to challenge a confidentiality designation by electing not to mount a challenge promptly after the original designation is disclosed.

Meet and Confer. The Challenging Party shall initiate the dispute resolution process by providing written notice of the designations it is challenging and generally describing the basis for the challenges. To avoid ambiguity as to whether a challenge has been made, the written notice must recite that the challenge to confidentiality is being made in accordance with this specific paragraph of the Protective Order. The parties shall attempt to resolve each challenge in good faith and must begin the process by conferring directly (in voice to voice dialogue; other forms of communication are not sufficient) within 10 days of the date of service of notice. In conferring, the Challenging Party must explain the basis for its belief that the confidentiality designation was not proper and must give the Designating Party an opportunity to review the designated material, to reconsider the circumstances, and, if no change in designation is offered, to explain the basis for the chosen designation. A Challenging Party may proceed to the next stage of the challenge process only if it has engaged in this meet and confer process first or establishes that the Designating Party is unwilling to participate in the meet and confer process in a timely manner.

Judicial Intervention. If the Parties cannot resolve a challenge without court intervention through the procedure set forth above, they must hold an informal in-person conference with the Court. If the Parties still cannot resolve the challenge, the Designating Party shall file and serve a motion to retain

confidentiality within 10 days of the informal in-person conference. Each such motion must be accompanied by a competent declaration affirming that the movant has complied with the meet and confer requirements imposed in the preceding paragraph. Failure by the Designating Party to timely make such a motion shall automatically waive the confidentiality designation for each challenged designation. In addition, the Challenging Party may file a motion challenging a confidentiality designation at any time if there is good cause for doing so, including a challenge to the designation of a deposition transcript or any portions thereof. Any motion brought pursuant to this provision must be accompanied by a competent declaration affirming that the movant has complied with the meet and confer requirements imposed by the preceding paragraph. The burden of persuasion in any such challenge proceeding shall be on the Designating Party. The Court recommends that the parties obtain a court reporter for the hearing on this motion. Frivolous challenges, and those made for an improper purpose (e.g., to harass or impose unnecessary expenses and burdens on other parties) may expose the Challenging Party to sanctions. The party losing any motion concerning the confidentiality of materials will pay the successful party's attorneys' fees incurred in the making of or opposing the motion if the losing position was not substantially justified. Unless the Designating Party has waived the confidentiality designation by failing to file a motion to retain confidentiality as described above, all parties shall continue to afford the material in question the level of protection to which it is entitled under the Producing Party's designation until the court rules on the challenge.

CERTIFICATE OF ELECTRONIC SERVICE
(CCP 1010.6(6) & CRC 2.260(g))

I, Felicia Green, a Deputy Clerk of the Superior Court of the County of San Francisco, certify that I am not a party to the within action.

On March 2, 2023, I electronically served ORDER CONTINUING MARCH 7, 2023 CASE MANAGEMENT CONFERENCE via File & ServeXpress on the recipients designated on the Transaction Receipt located on the File & ServeXpress website.

Dated: MAR 02 2023

Mark Culkins, Interim Chief Executive Officer of the Court

By: Felicia Green
Felicia Green, Deputy Clerk

SUPERIOR COURT OF CALIFORNIA
COUNTY OF SAN FRANCISCO

400 MCALLISTER STREET, SAN FRANCISCO, CA 94102-4514

MY CHOICE SOFTWARE, LLC,

PLAINTIFF (S)

VS.

SHOPIFY, INC., A CANADIAN CORPORATION et al

DEFENDANT (S)

Department 304

NO.: CGC-22-601842

Order Granting Complex Designation and for Single Assignment

TO: ALL COUNSEL AND PARTIES IN PROPRIA PERSONA

The Application for Approval of Complex Designation filed Dec-08-2022, in the above-entitled action, is GRANTED. Complex Designation is APPROVED and this action is singly assigned for all purposes.

The CASE MANAGEMENT CONFERENCE previously set for Feb-15-2023 is canceled.

It is hereby ordered that this entire action be assigned for all purposes to the Complex Litigation Department, Judge Ethan P. Schulman, Department 304, of the California Superior Court for the County of San Francisco at 400 McAllister Street, San Francisco, CA 94102.

A case management conference is set for Feb-21-2023 at 10:00 am in Department 304. A JOINT case management statement must be filed and an endorsed copy thereof delivered to Department 304 no later than five (5) court days prior to the case management conference. All court dates must be reserved in advance with the Clerk of the Court. The Clerk of the Court in Department 304 may be contacted at (415) 551-3729.

Remote appearances are allowed through Court Call or Zoom. If appearing remotely, please meet and confer to decide which platform to use as appearances cannot be split between Zoom and Court Call due to sound interference. Should the parties wish to appear via Zoom, they are to jointly email the Complex Litigation Department at Complexlit@sftc.org to make that request. The request must include each attorney's name, firm, address, telephone number, email address and the name(s) of the client(s) each is representing. Upon receipt, the clerk will send a Zoom link for the conference.

All counsel should read and be familiar with the department procedures, a copy of which is enclosed, and are located online at: https://www.sfsuperiorcourt.org/divisions/civil/litigation.

Any pending motions previously set for hearing in the Law and Motion or Discovery Departments should be taken off calendar and the papers forwarded to Department 304 for possible re-setting at the time of the case management conference.

Counsel for plaintiff shall provide a copy of this order and notice to all counsel of record and/or parties In Propria Persona that are not listed in the attached certificate of service.

This case is now subject to mandatory e-filing and e-service pursuant to Local Rule 2.11. For e-filing registration, training information and service list assistance, contact the Court's approved e-filing & e-service provider at (888)529-7587.

DATED: DEC-28-2022

Ethan P. Schulman

JUDGE

Superior Court of California

County of San Francisco

Department 304 - Judge Ethan P. Schulman

Complex Litigation – Procedures

Department 304 Staff:

- Clerk: Ericka Larnauti
- Clerk Phone: 415-551-3729/5948
- Attorney: Kiara Canales
- Department 304 Email: complexlit@sftc.org

Communications with the Court and Reserving Hearing Dates:

- Prior to filing any motion, all motion hearing dates must be reserved with the clerk of Department 304. Parties may not file a motion without Court approval of the hearing date and time.
- Generally, the clerk of Department 304 prefers email communications. If a party emails the clerk, they must include all counsel on the email.

Continuances:

- If the parties wish to continue a motion or a CMC, the parties may (1) submit a stipulation and proposed order; or (2) email the Court (copying all parties) at least three court days prior to the scheduled matter requesting a continuance and indicating that all parties agree to the continued date/time.

Hearing Date Vacated by Party:

- If a moving party removes a motion from the Court's calendar (either on its own, or by submitting to the Court's tentative ruling on the motion), the party must notify all other parties by email or telephone.

Appearances:

- Counsel may appear for hearings in person, via Zoom, or via CourtCall. Should the parties wish to appear via Zoom, they are to jointly email the Complex Litigation Department to make that request. The request must include each attorney's name, firm, address, telephone number, and email address and the name(s) of the client(s) each is representing. Upon receipt, the clerk will send a Zoom link for the conference. The parties may not split an appearance via Zoom and CourtCall due to sound interference.

Discovery:

- The procedures outlined below apply only to parties. With regard to discovery disputes with non-parties, the interested parties may elect to participate in this procedure, but are not required to do so.
- All deadlines for filing motions to compel discovery pursuant to the Civil Discovery Act, Code of Civil Procedure section 2016.010 *et seq.*, are vacated and suspended. No party may move to compel discovery, or file any other discovery motion, until the parties have had a discovery conference with the Court.
- Counsel must have completed all meet and confer obligations before scheduling a discovery conference.
- To request a discovery conference with the Court, counsel must contact the clerk of Department 304. Once a conference is scheduled, counsel are responsible for setting up a Zoom link or telephone conference line.
- At least three court days before the conference, counsel must email a **joint** letter outlining the discovery dispute, not exceeding 5 pages, single-spaced.
- If the discovery dispute is not resolved following the conference, any party may proceed to file a motion. Any such motion must be filed within 10 court days of the conference.
- The parties are relieved of the requirement to file a separate statement in discovery motions.
- For discovery motions, the Court prefers streamlined papers in which counsel state the discovery request and response followed by a discussion of whether a further response is or is not required. In lieu of the usual discovery motion briefing, the parties may instead provide one single filing that includes the question, the response and why more information is owed or not owed. The Court is open to the parties agreeing to an expedited briefing schedule where one side files a 5-page motion, the other side files a 5-page response, the moving party a 3-page reply and a hearing date is set 10 days out from the last filing.

E-Filing:

- The e-filing vendor for the San Francisco Superior Court Complex Department is File&Serve*Xpress*. Counsel must register with and submit all filings through said vendor. Counsel must also add themselves to the vendor's e-service list. Customer Service for e-filing registration, training information, and service list assistance can be found at support@fileandservexpress.com or by calling File&Serve*Xpress* at 888-529-7587.
- All court orders will be e-served through File&Serve*Xpress*. All counsel must add their office to the service list at File&Serve*Xpress*.
- Pursuant to California Code of Civil Procedure section 1010.6, California Rules of Court, rule 2.251 *et seq.*, and San Francisco Superior Court Local Rule 2.11, all discovery requests and responses, not filed with the court, must be electronically served, unless it is not feasible to do so (e.g., drawings, charts, etc.).
- Pursuant to Code of Civil Procedure section 1010.6(b)(3), any document received electronically by the court between 12:00 a.m. and 11:59:59 p.m. on a court day shall be deemed filed that day; any document received by a court on a non-court day will be deemed filed on the next court day.

- Pursuant to Code of Civil Procedure section 1010.6(a)(5), any document served electronically between 12:00 a.m. and 11:59:59 p.m. on a court day will be deemed served that day; any document electronically served on a non-court day will be deemed served the next court day.

Courtesy Copies:

- Counsel are directed to deliver two hard copies of all e-filed documents to Department 304, which includes proposed orders.

Challenging Confidentiality Designations:

- If the parties enter into a stipulation for a protective order, the protective order must include the language found in Attachment 1 governing the process for any party to challenge the confidentiality designation.

Sealing Motions:

- Regarding motions to seal, the Court reminds counsel to follow California Rules of Court, rules 2.550-2.551. These requirements do not apply to discovery motions but do apply to all other types of motions. Please do not submit sealed documents unless the parties need the Court to consider them. Please read *Overstock.Com, Inc. v. Goldman Sachs Grp., Inc.* (2014) 231 Cal.App.4th 471. The Court is required to follow the California Rules of Court and make specific findings.
- For motions to seal (and accompanied unredacted versions of documents conditionally lodged under seal with the Court,) the parties must highlight in yellow the proposed sealing request in the unredacted documents.

Tentative Rulings:

- For most motions, tentative rulings will be emailed directly to counsel prior to the hearing.

Court Reporters:

- The Court does not provide court reporters for hearings.
- The Court recommends that the parties obtain court reporters for substantive motions.
- The Court requests that the parties arrange for the Court to be provided with hearing transcripts following substantive motions. This is not required.

CMC Statements:

- A joint case management conference statement must be filed, and two copies delivered to Department 304, no later than five court days prior to the case management conference. Individual statements will not be considered. Do not use the Judicial Council form for case management conference statements.

- The purpose of the joint statement is that it requires counsel to confer. It shows the Court that the parties have been in direct communication.
- CMC statements are not advocacy statements. They are an agenda for a discussion. CMC statements should explain where the case is, where it is going, and how it can most efficiently reach its destination.

SUPERIOR COURT OF CALIFORNIA

COUNTY OF SAN FRANCISCO

COMPLEX LITIGATION

CHALLENGING CONFIDENTIALITY DESIGNATIONS

Timing of Challenges. Any Party or Non-Party may challenge a designation of confidentiality at any time. Unless a prompt challenge to a Designating Party's confidentiality designation is necessary to avoid foreseeable, substantial unfairness, unnecessary economic burdens, or a significant disruption or delay of the litigation, a Party does not waive its right to challenge a confidentiality designation by electing not to mount a challenge promptly after the original designation is disclosed.

Meet and Confer. The Challenging Party shall initiate the dispute resolution process by providing written notice of the designations it is challenging and generally describing the basis for the challenges. To avoid ambiguity as to whether a challenge has been made, the written notice must recite that the challenge to confidentiality is being made in accordance with this specific paragraph of the Protective Order. The parties shall attempt to resolve each challenge in good faith and must begin the process by conferring directly (in voice to voice dialogue; other forms of communication are not sufficient) within 10 days of the date of service of notice. In conferring, the Challenging Party must explain the basis for its belief that the confidentiality designation was not proper and must give the Designating Party an opportunity to review the designated material, to reconsider the circumstances, and, if no change in designation is offered, to explain the basis for the chosen designation. A Challenging Party may proceed to the next stage of the challenge process only if it has engaged in this meet and confer process first or establishes that the Designating Party is unwilling to participate in the meet and confer process in a timely manner.

Judicial Intervention. If the Parties cannot resolve a challenge without court intervention through the procedure set forth above, they must hold an informal in-person conference with the Court. If the Parties still cannot resolve the challenge, the Designating Party shall file and serve a motion to retain

confidentiality within 10 days of the informal in-person conference. Each such motion must be accompanied by a competent declaration affirming that the movant has complied with the meet and confer requirements imposed in the preceding paragraph. Failure by the Designating Party to timely make such a motion shall automatically waive the confidentiality designation for each challenged designation. In addition, the Challenging Party may file a motion challenging a confidentiality designation at any time if there is good cause for doing so, including a challenge to the designation of a deposition transcript or any portions thereof. Any motion brought pursuant to this provision must be accompanied by a competent declaration affirming that the movant has complied with the meet and confer requirements imposed by the preceding paragraph. The burden of persuasion in any such challenge proceeding shall be on the Designating Party. The Court recommends that the parties obtain a court reporter for the hearing on this motion. Frivolous challenges, and those made for an improper purpose (e.g., to harass or impose unnecessary expenses and burdens on other parties) may expose the Challenging Party to sanctions. The party losing any motion concerning the confidentiality of materials will pay the successful party's attorneys' fees incurred in the making of or opposing the motion if the losing position was not substantially justified. Unless the Designating Party has waived the confidentiality designation by failing to file a motion to retain confidentiality as described above, all parties shall continue to afford the material in question the level of protection to which it is entitled under the Producing Party's designation until the court rules on the challenge.

POS-015

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name, State Bar number, and address)
RICHARD E. QUINTILONE II, ESQ. (SBN: 200995)
QUINTILONE & ASSOCIATES
22974 El Toro Road #100, Lake Forest, CA 92630
TELEPHONE NO. (949) 458-9675 FAX NO. (Optional)
E-MAIL ADDRESS (Optional): req@quintlaw.com
ATTORNEY FOR (Name): Plaintiff, MY CHOICE SOFTWARE, LLC, et al.

FOR COURT USE ONLY

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SAN FRANCISCO
STREET ADDRESS: 400 McAllister Street
MAILING ADDRESS:
CITY AND ZIP CODE: San Francisco, CA 94102
BRANCH NAME: Civic Center Courthouse

PLAINTIFF/PETITIONER: MY CHOICE SOFTWARE, LLC, et al.

DEFENDANT/RESPONDENT: SHOPIFY, INC., et al.

NOTICE AND ACKNOWLEDGMENT OF RECEIPT—CIVIL

CASE NUMBER: CGC-22-601842

TO *(insert name of party being served)*: Shopify (USA) Inc., a Delaware Corporation

NOTICE

The summons and other documents identified below are being served pursuant to section 415.30 of the California Code of Civil Procedure. Your failure to complete this form and return it within 20 days from the date of mailing shown below may subject you (or the party on whose behalf you are being served) to liability for the payment of any expenses incurred in serving a summons on you in any other manner permitted by law.

If you are being served on behalf of a corporation, an unincorporated association (including a partnership), or other entity, this form must be signed by you in the name of such entity or by a person authorized to receive service of process on behalf of such entity. In all other cases, this form must be signed by you personally or by a person authorized by you to acknowledge receipt of summons. If you return this form to the sender, service of a summons is deemed complete on the day you sign the acknowledgment of receipt below.

Date of mailing: April 24, 2023

Richard E. Quintilone II, Esq.
(TYPE OR PRINT NAME)

▶ _____
(SIGNATURE OF SENDER—MUST NOT BE A PARTY IN THIS CASE)

ACKNOWLEDGMENT OF RECEIPT

This acknowledges receipt of ***(to be completed by sender before mailing)***:

1. ☑ A copy of the summons and of the complaint.
2. ☑ Other *(specify)*:
   1. Civil Case Cover Sheet;
   2. Order Granting Complex Designation;
   3. Order Continuing Case Management Conference;
   4. Notice of Related Case.

(To be completed by recipient):

Date this form is signed:

_____
(TYPE OR PRINT YOUR NAME AND NAME OF ENTITY, IF ANY, ON WHOSE BEHALF THIS FORM IS SIGNED)

▶ _____
(SIGNATURE OF PERSON ACKNOWLEDGING RECEIPT, WITH TITLE IF ACKNOWLEDGMENT IS MADE ON BEHALF OF ANOTHER PERSON OR ENTITY)

Form Adopted for Mandatory Use
Judicial Council of California
POS-015 [Rev. January 1, 2005]

NOTICE AND ACKNOWLEDGMENT OF RECEIPT — CIVIL

Code of Civil Procedure
§§ 415.30, 417.10
www.courtinfo.ca.gov

American LegalNet, Inc.
www.USCourtForms.com

POS-015

ATTORNEY OR PARTY WITHOUT ATTORNEY (Name, State Bar number, and address):
RICHARD E. QUINTILONE II, ESQ. (SBN: 200995)
QUINTILONE & ASSOCIATES
22974 El Toro Road #100, Lake Forest, CA 92630
TELEPHONE NO. (949) 458-9675 FAX NO. (Optional):
E-MAIL ADDRESS (Optional): req@quintlaw.com
ATTORNEY FOR (Name): Plaintiff, MY CHOICE SOFTWARE, LLC, et al.

FOR COURT USE ONLY

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SAN FRANCISCO
STREET ADDRESS: 400 McAllister Street
MAILING ADDRESS:
CITY AND ZIP CODE: San Francisco, CA 94102
BRANCH NAME: Civic Center Courthouse

PLAINTIFF/PETITIONER: MY CHOICE SOFTWARE, LLC, et al.

DEFENDANT/RESPONDENT: SHOPIFY, INC., et al.

NOTICE AND ACKNOWLEDGMENT OF RECEIPT—CIVIL

CASE NUMBER: CGC-22-601842

TO *(insert name of party being served)*: Shopify Inc., a Canadian Corporation

NOTICE

The summons and other documents identified below are being served pursuant to section 415.30 of the California Code of Civil Procedure. Your failure to complete this form and return it within 20 days from the date of mailing shown below may subject you (or the party on whose behalf you are being served) to liability for the payment of any expenses incurred in serving a summons on you in any other manner permitted by law.

If you are being served on behalf of a corporation, an unincorporated association (including a partnership), or other entity, this form must be signed by you in the name of such entity or by a person authorized to receive service of process on behalf of such entity. In all other cases, this form must be signed by you personally or by a person authorized by you to acknowledge receipt of summons. If you return this form to the sender, service of a summons is deemed complete on the day you sign the acknowledgment of receipt below.

Date of mailing: April 24, 2023

Richard E. Quintilone II, Esq.
(TYPE OR PRINT NAME)

▶ _____
(SIGNATURE OF SENDER—MUST NOT BE A PARTY IN THIS CASE)

ACKNOWLEDGMENT OF RECEIPT

This acknowledges receipt of ***(to be completed by sender before mailing)***:

1. ☑ A copy of the summons and of the complaint.
2. ☑ Other *(specify)*:
   1. Civil Case Cover Sheet;
   2. Order Granting Complex Designation;
   3. Order Continuing Case Management Conference;
   4. Notice of Related Case.

(To be completed by recipient):

Date this form is signed:

_____
(TYPE OR PRINT YOUR NAME AND NAME OF ENTITY, IF ANY, ON WHOSE BEHALF THIS FORM IS SIGNED)

▶ _____
(SIGNATURE OF PERSON ACKNOWLEDGING RECEIPT, WITH TITLE IF ACKNOWLEDGMENT IS MADE ON BEHALF OF ANOTHER PERSON OR ENTITY)

Form Adopted for Mandatory Use
Judicial Council of California
POS-015 [Rev. January 1, 2005]

NOTICE AND ACKNOWLEDGMENT OF RECEIPT — CIVIL

Code of Civil Procedure
§§ 415.30, 417.10
www.courtinfo.ca.gov